aws

Panduan Developerr

AWS Encryption SDK

AWS Encryption SDK: Panduan Developerr

Table of Contents

Apa itu AWS Encryption SDK?

AWS Encryption SDK Ini adalah pustaka enkripsi sisi klien yang dirancang untuk memudahkan semua orang mengenkripsi dan mendekripsi data menggunakan standar industri dan praktik terbaik. Ini memungkinkan Anda untuk fokus pada fungsionalitas inti aplikasi Anda, bukan pada cara terbaik mengenkripsi dan mendekripsi data Anda. AWS Encryption SDK Ini disediakan secara gratis di bawah lisensi Apache 2.0.

AWS Encryption SDK Jawaban pertanyaan-pertanyaan seperti berikut untuk Anda:

- Algoritma enkripsi mana yang harus saya gunakan?
- Bagaimana, atau dalam mode apa, saya harus menggunakan algoritma itu?
- Bagaimana cara menghasilkan kunci enkripsi?
- Bagaimana cara melindungi kunci enkripsi, dan di mana saya harus menyimpannya?
- Bagaimana saya bisa membuat data terenkripsi saya portabel?
- Bagaimana cara memastikan bahwa penerima yang dituju dapat membaca data terenkripsi saya?
- Bagaimana saya bisa memastikan data terenkripsi saya tidak dimodifikasi antara waktu ditulis dan ketika dibaca?
- Bagaimana cara menggunakan kunci data yang AWS KMS kembali?

Dengan AWS Encryption SDK, Anda menentukan penyedia kunci master atau keyring yang menentukan kunci pembungkus yang Anda gunakan untuk melindungi data Anda. Kemudian Anda mengenkripsi dan mendekripsi data Anda menggunakan metode langsung yang disediakan oleh. AWS Encryption SDK Yang AWS Encryption SDK melakukan sisanya.

Tanpa itu AWS Encryption SDK, Anda mungkin menghabiskan lebih banyak upaya untuk membangun solusi enkripsi daripada fungsionalitas inti aplikasi Anda. AWS Encryption SDK Jawaban pertanyaan-pertanyaan ini dengan memberikan hal-hal berikut.

Implementasi default yang mematuhi praktik terbaik kriptografi

> Secara default, AWS Encryption SDK menghasilkan kunci data unik untuk setiap objek data yang dienkripsi. Ini mengikuti praktik terbaik kriptografi menggunakan kunci data unik untuk setiap operasi enkripsi.

AWS Encryption SDK Enkripsi data Anda menggunakan algoritma kunci simetris yang aman, terautentikasi. Untuk informasi selengkapnya, lihat the section called “Suite algoritma yang didukung”.

Kerangka kerja untuk melindungi kunci data dengan kunci pembungkus

Ini AWS Encryption SDK melindungi kunci data yang mengenkripsi data Anda dengan mengenkripsi mereka di bawah satu atau lebih kunci pembungkus. Dengan menyediakan kerangka kerja untuk mengenkripsi kunci data dengan lebih dari satu kunci pembungkus, AWS Encryption SDK membantu membuat data terenkripsi Anda portabel.

Misalnya, mengenkripsi data di bawah kunci AWS KMS key masuk AWS KMS dan kunci dari HSM lokal Anda. Anda dapat menggunakan salah satu kunci pembungkus untuk mendekripsi data, jika salah satu tidak tersedia atau pemanggil tidak memiliki izin untuk menggunakan kedua kunci.

Pesan diformat yang menyimpan kunci data terenkripsi dengan data terenkripsi

AWS Encryption SDK Menyimpan data terenkripsi dan kunci data terenkripsi bersama-sama dalam pesan terenkripsi yang menggunakan format data yang ditentukan. Ini berarti Anda tidak perlu melacak atau melindungi kunci data yang mengenkripsi data Anda karena AWS Encryption SDK melakukannya untuk Anda.

Beberapa implementasi bahasa AWS Encryption SDK memerlukan AWS SDK, tetapi AWS Encryption SDK tidak memerlukan Akun AWS dan tidak bergantung pada layanan apa pun AWS . Anda Akun AWS hanya perlu jika Anda memilih untuk menggunakan AWS KMS keysuntuk melindungi data Anda.

Dikembangkan dalam repositori sumber terbuka

AWS Encryption SDK Ini dikembangkan dalam repositori sumber terbuka di. GitHub Anda dapat menggunakan repositori ini untuk melihat kode, membaca dan mengirimkan masalah, dan menemukan informasi yang spesifik untuk implementasi bahasa Anda.

- AWS Encryption SDK for C — aws-encryption-sdk-c
- AWS Encryption SDK untuk direktori.NET — .NET dari `aws-encryption-sdk` repositori.
- AWS Enkripsi CLI — aws-encryption-sdk-cli
- AWS Encryption SDK for Java — aws-encryption-sdk-java

- AWS Encryption SDK for JavaScript — aws-encryption-sdk-javascript
- AWS Encryption SDK for Python — aws-encryption-sdk-python
- AWS Encryption SDK untuk direktori Rust — Rust dari `aws-encryption-sdk` repositori.
- AWS Encryption SDK untuk direktori Go — Go dari `aws-encryption-sdk` repositori

Kompatibilitas dengan pustaka dan layanan enkripsi

AWS Encryption SDK Ini didukung dalam beberapa bahasa pemrograman. Semua implementasi bahasa dapat dioperasikan secara interoperable. Anda dapat mengenkripsi dengan satu implementasi bahasa dan mendekripsi dengan yang lain. Interoperabilitas mungkin tunduk pada kendala bahasa. Jika demikian, kendala ini dijelaskan dalam topik tentang implementasi bahasa. Selain itu, saat mengenkripsi dan mendekripsi, Anda harus menggunakan keyring yang kompatibel, atau kunci master dan penyedia kunci master. Lihat perinciannya di the section called “Kompatibilitas keyring”.

Namun, AWS Encryption SDK tidak dapat beroperasi dengan perpustakaan lain. Karena setiap pustaka mengembalikan data terenkripsi dalam format yang berbeda, Anda tidak dapat mengenkripsi dengan satu pustaka dan mendekripsi dengan yang lain.

Klien Enkripsi DynamoDB dan enkripsi sisi klien Amazon S3

> AWS Encryption SDK Tidak dapat mendekripsi data yang dienkripsi oleh Klien Enkripsi DynamoDB atau enkripsi sisi klien Amazon S3. Pustaka ini tidak dapat mendekripsi pesan terenkripsi yang dikembalikan. AWS Encryption SDK

AWS Key Management Service (AWS KMS)

> AWS Encryption SDK Dapat menggunakan AWS KMS keysdan kunci data untuk melindungi data Anda, termasuk kunci KMS Multi-wilayah. Misalnya, Anda dapat mengonfigurasi AWS Encryption SDK untuk mengenkripsi data Anda di bawah satu atau lebih AWS KMS keys di file Anda Akun AWS. Namun, Anda harus menggunakan AWS Encryption SDK untuk mendekripsi data tersebut.
>
> AWS Encryption SDK Tidak dapat mendekripsi ciphertext yang dikembalikan AWS KMS Enkripsi atau operasi. ReEncrypt Demikian pula, operasi AWS KMS Dekripsi tidak dapat mendekripsi pesan terenkripsi yang dikembalikan. AWS Encryption SDK
>
> Hanya AWS Encryption SDK mendukung kunci KMS enkripsi simetris. Anda tidak dapat menggunakan kunci KMS asimetris untuk enkripsi atau masuk. AWS Encryption SDK Ini AWS

Encryption SDK menghasilkan kunci penandatanganan ECDSA sendiri untuk rangkaian algoritme yang menandatangani pesan.

Support dan pemeliharaan

AWS Encryption SDK Menggunakan kebijakan pemeliharaan yang sama dengan yang digunakan AWS SDK dan Tools, termasuk fase pembuatan versi dan siklus hidupnya. Sebagai praktik terbaik, kami menyarankan Anda menggunakan versi terbaru yang tersedia AWS Encryption SDK untuk bahasa pemrograman Anda, dan meningkatkan saat versi baru dirilis. Ketika versi memerlukan perubahan signifikan, seperti upgrade dari AWS Encryption SDK versi lebih awal dari 1.7. x ke versi 2.0. x dan yang lebih baru, kami memberikan instruksi terperinci untuk membantu Anda.

Setiap implementasi bahasa AWS Encryption SDK pemrograman dikembangkan dalam GitHub repositori open-source terpisah. Siklus hidup dan fase dukungan dari setiap versi cenderung bervariasi di antara repositori. Misalnya, versi yang diberikan AWS Encryption SDK mungkin berada dalam fase ketersediaan umum (dukungan penuh) dalam satu bahasa pemrograman, tetapi end-of-support fase dalam bahasa pemrograman yang berbeda. Kami menyarankan Anda menggunakan versi yang didukung sepenuhnya bila memungkinkan dan menghindari versi yang tidak lagi didukung.

Untuk menemukan fase siklus hidup AWS Encryption SDK versi untuk bahasa pemrograman Anda, lihat `SUPPORT_POLICY.rst` file di setiap AWS Encryption SDK repositori.

- AWS Encryption SDK for C — Support_Policy.rst
- AWS Encryption SDK untuk .NET — SUPPORT_POLICY.RST
- AWS Enkripsi CLI — SUPPORT_POLICY.RST
- AWS Encryption SDK for Java — Support_Policy.rst
- AWS Encryption SDK for JavaScript — Support_Policy.rst
- AWS Encryption SDK for Python — Support_Policy.rst

Untuk informasi selengkapnya, lihat Versi dari AWS Encryption SDK AWS SDKs dan serta Kebijakan pemeliharaan alat di Panduan Referensi Alat AWS SDKs dan Alat.

Belajar lebih

Untuk informasi lebih lanjut tentang enkripsi sisi klien AWS Encryption SDK dan enkripsi, coba sumber-sumber ini.

- Untuk bantuan mengenai istilah dan konsep yang digunakan dalam SDK ini, lihatKonsep dalam AWS Encryption SDK.
- Untuk pedoman praktik terbaik, lihatPraktik terbaik untuk AWS Encryption SDK.
- Untuk informasi tentang cara kerja SDK ini, lihatCara kerja SDK.
- Untuk contoh yang menunjukkan cara mengkonfigurasi opsi di AWS Encryption SDK, lihatMengkonfigurasi AWS Encryption SDK.
- Untuk informasi teknis terperinci, lihatReferensi.
- Untuk spesifikasi teknis AWS Encryption SDK, lihat AWS Encryption SDK Spesifikasi di GitHub.
- Untuk jawaban atas pertanyaan Anda tentang penggunaan AWS Encryption SDK, baca dan posting di Forum Diskusi Alat AWS Crypto.

Untuk informasi tentang implementasi dari AWS Encryption SDK dalam bahasa pemrograman yang berbeda.

- C: LihatAWS Encryption SDK for C, dokumentasi AWS Encryption SDK C, dan aws-encryption-sdk-crepositori aktif. GitHub
- C#/.NET: Lihat AWS Encryption SDK untuk .NET dan aws-encryption-sdk-netdirektori repositori aktif. `aws-encryption-sdk` GitHub
- Antarmuka Baris Perintah: LihatAWS Encryption SDK antarmuka baris perintah, Baca Dokumen untuk CLI AWS Enkripsi, dan aws-encryption-sdk-clirepositori aktif. GitHub
- Java: LihatAWS Encryption SDK for Java, AWS Encryption SDK Javadoc, dan aws-encryption-sdk-javarepositori aktif. GitHub

  JavaScript: Lihat the section called “JavaScript” dan aws-encryption-sdk-javascriptrepositori aktif. GitHub
- Python: LihatAWS Encryption SDK for Python, dokumentasi AWS Encryption SDK Python, dan repositori aktif. aws-encryption-sdk-python GitHub

Mengirim umpan balik

Kami menyambut umpan balik Anda! Jika Anda memiliki pertanyaan atau komentar, atau masalah yang perlu dilaporkan, silakan gunakan sumber daya berikut.

- Jika Anda menemukan potensi kerentanan keamanan di AWS Encryption SDK, harap beri tahu AWS keamanan. Jangan membuat GitHub masalah publik.

- Untuk memberikan umpan balik tentang AWS Encryption SDK, ajukan masalah di GitHub repositori untuk bahasa pemrograman yang Anda gunakan.
- Untuk memberikan umpan balik tentang dokumentasi ini, gunakan tautan Umpan Balik di halaman ini. Anda juga dapat mengajukan masalah atau berkontribusi pada aws-encryption-sdk-docs, repositori sumber terbuka untuk dokumentasi ini. GitHub

Konsep dalam AWS Encryption SDK

Bagian ini memperkenalkan konsep yang digunakan dalam AWS Encryption SDK, dan memberikan glosarium dan referensi. Ini dirancang untuk membantu Anda memahami cara AWS Encryption SDK kerja dan istilah yang kami gunakan untuk menggambarkannya.

Butuh bantuan?

- Pelajari cara AWS Encryption SDK menggunakan enkripsi amplop untuk melindungi data Anda.
- Pelajari tentang elemen enkripsi amplop: kunci data yang melindungi data Anda dan kunci pembungkus yang melindungi kunci data Anda.
- Pelajari tentang keyrings dan penyedia kunci utama yang menentukan kunci pembungkus yang Anda gunakan.
- Pelajari tentang konteks enkripsi yang menambahkan integritas pada proses enkripsi Anda. Ini opsional, tetapi ini adalah praktik terbaik yang kami rekomendasikan.
- Pelajari tentang pesan terenkripsi yang dikembalikan oleh metode enkripsi.
- Kemudian Anda siap untuk menggunakan AWS Encryption SDK dalam bahasa pemrograman pilihan Anda.

Topik

- Manajer materi kriptografi
- Enkripsi simetris dan asimetris
- Komitmen utama
- Kebijakan komitmen
- Tanda tangan digital

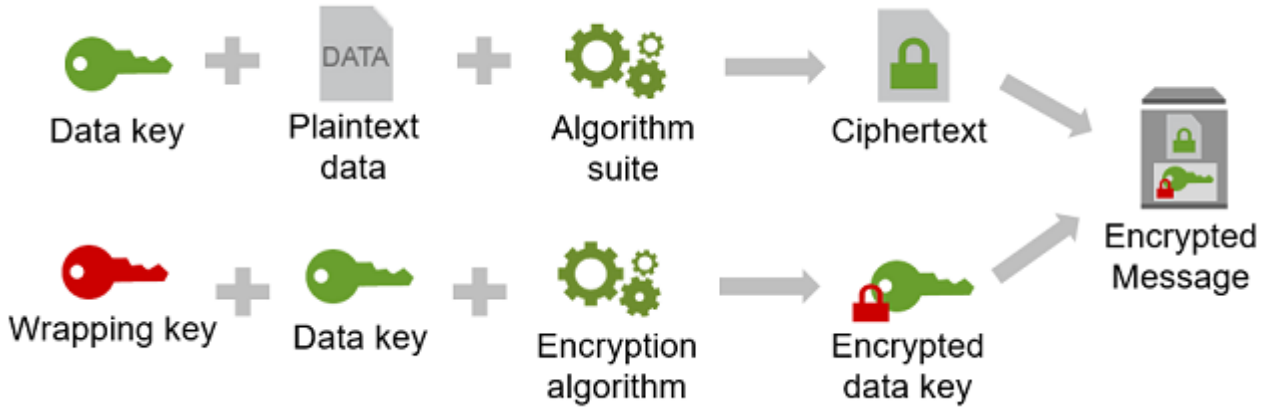
Enkripsi amplop

Keamanan data terenkripsi Anda sebagian bergantung pada perlindungan kunci data yang dapat mendekripsi itu. Salah satu praktik terbaik yang diterima untuk melindungi kunci data adalah mengenkripsinya. Untuk melakukan ini, Anda memerlukan kunci enkripsi lain, yang dikenal sebagai kunci enkripsi kunci atau kunci pembungkus. Praktek menggunakan kunci pembungkus untuk mengenkripsi kunci data dikenal sebagai enkripsi amplop.

Melindungi kunci data

AWS Encryption SDK Enkripsi setiap pesan dengan kunci data yang unik. Kemudian mengenkripsi kunci data di bawah kunci pembungkus yang Anda tentukan. Ini menyimpan kunci data terenkripsi dengan data terenkripsi dalam pesan terenkripsi yang dikembalikan.

Untuk menentukan kunci pembungkus Anda, Anda menggunakan keyring atau penyedia kunci master.

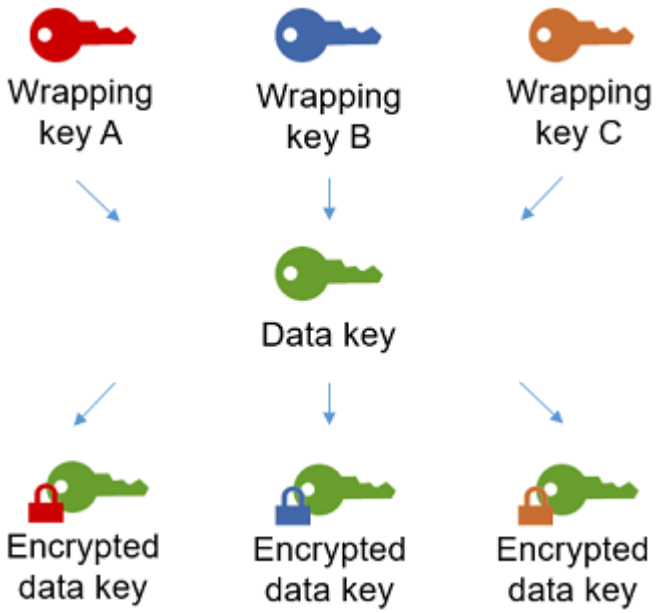


Mengenkripsi data yang sama di bawah beberapa kunci pembungkus

Anda dapat mengenkripsi kunci data di bawah beberapa kunci pembungkus. Anda mungkin ingin memberikan kunci pembungkus yang berbeda untuk pengguna yang berbeda, atau kunci

pembungkus dari jenis yang berbeda, atau di lokasi yang berbeda. Setiap kunci pembungkus mengenkripsi kunci data yang sama. AWS Encryption SDK Menyimpan semua kunci data terenkripsi dengan data terenkripsi dalam pesan terenkripsi.

Untuk mendekripsi data, Anda perlu menyediakan kunci pembungkus yang dapat mendekripsi salah satu kunci data terenkripsi.



Menggabungkan kekuatan dari beberapa algoritme

Untuk mengenkripsi data Anda, secara default, AWS Encryption SDK menggunakan rangkaian algoritma canggih dengan enkripsi simetris AES-GCM, fungsi derivasi kunci (HKDF), dan penandatanganan. Untuk mengenkripsi kunci data, Anda dapat menentukan algoritma enkripsi simetris atau asimetris yang sesuai dengan kunci pembungkus Anda.

Secara umum, algoritma enkripsi kunci simetris lebih cepat dan menghasilkan ciphertext yang lebih kecil daripada enkripsi kunci asimetris atau publik. Namun algoritme kunci publik memberikan pemisahan peran yang melekat dan manajemen kunci yang lebih mudah. Untuk menggabungkan kekuatan masing-masing, Anda dapat mengenkripsi data Anda dengan enkripsi kunci simetris, dan kemudian mengenkripsi kunci data dengan enkripsi kunci publik.

Kunci data

Kunci data adalah kunci enkripsi yang AWS Encryption SDK digunakan untuk mengenkripsi data Anda. Setiap kunci data adalah array byte yang sesuai dengan persyaratan untuk kunci kriptografi.

Kecuali Anda menggunakan caching kunci data, AWS Encryption SDK menggunakan kunci data unik untuk mengenkripsi setiap pesan.

Anda tidak perlu menentukan, menghasilkan, mengimplementasikan, memperluas, melindungi, atau menggunakan kunci data. AWS Encryption SDK Apakah itu bekerja untuk Anda ketika Anda memanggil operasi enkripsi dan dekripsi.

Untuk melindungi kunci data Anda, AWS Encryption SDK mengenkripsi mereka di bawah satu atau beberapa kunci enkripsi kunci yang dikenal sebagai kunci pembungkus atau kunci master. Setelah AWS Encryption SDK menggunakan kunci data plaintext Anda untuk mengenkripsi data Anda, itu akan menghapusnya dari memori sesegera mungkin. Kemudian menyimpan kunci data terenkripsi dengan data terenkripsi dalam pesan terenkripsi yang dikembalikan oleh operasi enkripsi. Lihat perinciannya di the section called “Cara kerja SDK”.

> **Tip**
>
> Dalam AWS Encryption SDK, kami membedakan kunci data dari kunci enkripsi data. Beberapa suite algoritma yang didukung, termasuk suite default, menggunakan fungsi derivasi kunci yang mencegah kunci data mencapai batas kriptografinya. Fungsi derivasi kunci mengambil kunci data sebagai input dan mengembalikan kunci enkripsi data yang sebenarnya digunakan untuk mengenkripsi data. Untuk alasan ini, kita sering mengatakan bahwa data dienkripsi “di bawah” kunci data daripada “oleh” kunci data.

Setiap kunci data terenkripsi mencakup metadata, termasuk pengidentifikasi kunci pembungkus yang mengenkripsi itu. Metadata ini memudahkan untuk mengidentifikasi kunci pembungkus yang valid saat AWS Encryption SDK mendekripsi.

Kunci pembungkus

Kunci pembungkus adalah kunci enkripsi kunci yang AWS Encryption SDK digunakan untuk mengenkripsi kunci data yang mengenkripsi data Anda. Setiap kunci data plaintext dapat dienkripsi di bawah satu atau lebih kunci pembungkus. Anda menentukan kunci pembungkus mana yang digunakan untuk melindungi data Anda saat mengonfigurasi keyring atau penyedia kunci utama.

> **Note**
>
> Kunci pembungkus mengacu pada kunci di keyring atau penyedia kunci master. Kunci master biasanya dikaitkan dengan `MasterKey` kelas yang Anda buat instance saat Anda menggunakan penyedia kunci master.

Ini AWS Encryption SDK mendukung beberapa kunci pembungkus yang umum digunakan, seperti AWS Key Management Service (AWS KMS) simetris AWS KMS keys(termasuk kunci KMS Multi-wilayah), kunci mentah AES-GCM (Advanced Encryption Standard/Galois Counter Mode), dan kunci RSA mentah. Anda juga dapat memperluas atau mengimplementasikan kunci pembungkus Anda sendiri.

Saat Anda menggunakan enkripsi amplop, Anda perlu melindungi kunci pembungkus Anda dari akses yang tidak sah. Anda dapat melakukan ini dengan salah satu cara berikut:

- Gunakan layanan web yang dirancang untuk tujuan ini, seperti AWS Key Management Service (AWS KMS).
- Gunakan modul keamanan perangkat keras (HSM) seperti yang ditawarkan oleh AWS CloudHSM.
- Gunakan alat dan layanan manajemen kunci lainnya.

Jika Anda tidak memiliki sistem manajemen kunci, kami sarankan AWS KMS. AWS Encryption SDK Terintegrasi dengan AWS KMS untuk membantu Anda melindungi dan menggunakan kunci pembungkus Anda. Namun, AWS Encryption SDK tidak memerlukan AWS atau AWS layanan apa pun.

Gantungan kunci dan penyedia kunci utama

Untuk menentukan kunci pembungkus yang Anda gunakan untuk enkripsi dan dekripsi, Anda menggunakan keyring atau penyedia kunci utama. Anda dapat menggunakan keyrings dan penyedia kunci master yang AWS Encryption SDK menyediakan atau merancang implementasi Anda sendiri. AWS Encryption SDK Menyediakan keyrings dan penyedia kunci master yang kompatibel satu sama lain tunduk pada kendala bahasa. Lihat perinciannya di Kompatibilitas keyring.

Sebuah keyring menghasilkan, mengenkripsi, dan mendekripsi kunci data. Saat Anda menentukan keyring, Anda dapat menentukan kunci pembungkus yang mengenkripsi kunci data Anda. Kebanyakan keyrings menentukan setidaknya satu kunci pembungkus atau layanan yang menyediakan dan melindungi kunci pembungkus. Anda juga dapat menentukan keyring tanpa

tombol pembungkus atau keyring yang lebih kompleks dengan opsi konfigurasi tambahan. Untuk bantuan memilih dan menggunakan gantungan kunci yang AWS Encryption SDK didefinisikan, lihat. Gantungan kunci

Keyrings didukung dalam bahasa pemrograman berikut:

- AWS Encryption SDK for C
- AWS Encryption SDK for JavaScript
- AWS Encryption SDK untuk .NET
- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.
- Versi 1. x dari AWS Encryption SDK untuk Rust
- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Penyedia kunci master adalah alternatif untuk keyring. Penyedia kunci master mengembalikan kunci pembungkus (atau kunci master) yang Anda tentukan. Setiap kunci master dikaitkan dengan satu penyedia kunci master, tetapi penyedia kunci master biasanya menyediakan beberapa kunci master. Penyedia kunci master didukung di Java, Python, dan AWS CLI Enkripsi.

Anda harus menentukan keyring (atau penyedia kunci utama) untuk enkripsi. Anda dapat menentukan keyring yang sama (atau penyedia kunci utama), atau yang lain, untuk dekripsi. Saat mengenkripsi, AWS Encryption SDK menggunakan semua kunci pembungkus yang Anda tentukan untuk mengenkripsi kunci data. Saat mendekripsi, hanya AWS Encryption SDK menggunakan kunci pembungkus yang Anda tentukan untuk mendekripsi kunci data terenkripsi. Menentukan kunci pembungkus untuk dekripsi adalah opsional, tetapi ini adalah praktik terbaik. AWS Encryption SDK

Untuk detail tentang menentukan kunci pembungkus, lihat. Memilih tombol pembungkus

Konteks enkripsi

Untuk meningkatkan keamanan operasi kriptografi Anda, sertakan konteks enkripsi dalam semua permintaan untuk mengenkripsi data. Menggunakan konteks enkripsi adalah opsional, tetapi ini adalah praktik terbaik kriptografi yang kami rekomendasikan.

Konteks enkripsi adalah sekumpulan pasangan nama-nilai yang berisi data otentikasi tambahan non-rahasia yang sewenang-wenang. Konteks enkripsi dapat berisi data apa pun yang Anda pilih,

tetapi biasanya terdiri dari data yang berguna dalam pencatatan dan pelacakan, seperti data tentang jenis file, tujuan, atau kepemilikan. Saat Anda mengenkripsi data, konteks enkripsi terikat secara kriptografis ke data terenkripsi sehingga konteks enkripsi yang sama diperlukan untuk mendekripsi data. AWS Encryption SDK Termasuk konteks enkripsi dalam plaintext di header pesan terenkripsi yang dikembalikan.

Konteks enkripsi yang AWS Encryption SDK digunakan terdiri dari konteks enkripsi yang Anda tentukan dan public key pair yang ditambahkan oleh manajer bahan kriptografi (CMM). Secara khusus, setiap kali Anda menggunakan algoritma enkripsi dengan penandatanganan, CMM menambahkan pasangan nama-nilai ke konteks enkripsi yang terdiri dari nama cadangan`aws-crypto-public-key`, dan nilai yang mewakili kunci verifikasi publik. `aws-crypto-public-key`Nama dalam konteks enkripsi dicadangkan oleh AWS Encryption SDK dan tidak dapat digunakan sebagai nama dalam pasangan lain dalam konteks enkripsi. Untuk detailnya, lihat AAD di Referensi Format Pesan.

Contoh konteks enkripsi berikut terdiri dari dua pasangan konteks enkripsi yang ditentukan dalam permintaan dan public key pair yang ditambahkan CMM.

```
"Purpose"="Test", "Department"="IT", aws-crypto-public-key=<public key>
```

Untuk mendekripsi data, Anda meneruskan pesan terenkripsi. Karena AWS Encryption SDK dapat mengekstrak konteks enkripsi dari header pesan terenkripsi, Anda tidak diharuskan untuk menyediakan konteks enkripsi secara terpisah. Namun, konteks enkripsi dapat membantu Anda mengonfirmasi bahwa Anda mendekripsi pesan terenkripsi yang benar.

- Dalam AWS Encryption SDK Command Line Interface (CLI), jika Anda memberikan konteks enkripsi dalam perintah dekripsi, CLI memverifikasi bahwa nilai-nilai hadir dalam konteks enkripsi pesan terenkripsi sebelum mengembalikan data plaintext.
- Dalam implementasi bahasa pemrograman lainnya, respon dekripsi mencakup konteks enkripsi dan data plaintext. Fungsi dekripsi dalam aplikasi Anda harus selalu memverifikasi bahwa konteks enkripsi dalam respons dekripsi menyertakan konteks enkripsi dalam permintaan enkripsi (atau subset) sebelum mengembalikan data teks biasa.

> **Note**
>
> Versi berikut mendukung konteks enkripsi CMM yang diperlukan, yang dapat Anda gunakan untuk memerlukan konteks enkripsi di semua permintaan enkripsi.

- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK untuk .NET
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.
- Versi 1. x dari AWS Encryption SDK untuk Rust
- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Saat memilih konteks enkripsi, ingatlah bahwa itu bukan rahasia. Konteks enkripsi ditampilkan dalam plaintext di header pesan terenkripsi yang dikembalikan. AWS Encryption SDK Jika Anda menggunakan AWS Key Management Service, konteks enkripsi juga mungkin muncul dalam teks biasa dalam catatan audit dan log, seperti. AWS CloudTrail

Untuk contoh mengirimkan dan memverifikasi konteks enkripsi dalam kode Anda, lihat contoh untuk bahasa pemrograman pilihan Anda.

Pesan terenkripsi

Ketika Anda mengenkripsi data dengan AWS Encryption SDK, ia mengembalikan pesan terenkripsi.

Pesan terenkripsi adalah struktur data berformat portabel yang mencakup data terenkripsi bersama dengan salinan kunci data terenkripsi, ID algoritma, dan, secara opsional, konteks enkripsi dan tanda tangan digital. Enkripsi operasi dalam AWS Encryption SDK pengembalian pesan terenkripsi dan operasi dekripsi mengambil pesan terenkripsi sebagai input.

Menggabungkan data terenkripsi dan kunci data terenkripsi merampingkan operasi dekripsi dan membebaskan Anda dari keharusan menyimpan dan mengelola kunci data terenkripsi secara independen dari data yang mereka enkripsi.

Untuk informasi teknis tentang pesan terenkripsi, lihat Format Pesan Terenkripsi.

Suite algoritma

AWS Encryption SDK Menggunakan rangkaian algoritma untuk mengenkripsi dan menandatangani data dalam pesan terenkripsi yang dikembalikan oleh operasi enkripsi dan dekripsi. AWS Encryption SDK Mendukung beberapa suite algoritma. Semua suite yang didukung menggunakan Advanced Encryption Standard (AES) sebagai algoritma utama, dan menggabungkannya dengan algoritme dan nilai lainnya.

AWS Encryption SDK Menetapkan suite algoritma yang direkomendasikan sebagai default untuk semua operasi enkripsi. Default mungkin berubah seiring dengan peningkatan standar dan praktik terbaik. Anda dapat menentukan rangkaian algoritme alternatif dalam permintaan untuk mengenkripsi data atau saat membuat manajer bahan kriptografi (CMM), tetapi kecuali alternatif diperlukan untuk situasi Anda, yang terbaik adalah menggunakan default. Default saat ini adalah AES-GCM dengan fungsi derivasi extract-and-expand kunci berbasis HMAC (HKDF), komitmen utama, tanda tangan Elliptic Curve Digital Signature Algorithm (ECDSA), dan kunci enkripsi 256-bit.

Jika aplikasi Anda memerlukan kinerja tinggi dan pengguna yang mengenkripsi data dan mereka yang mendekripsi data sama-sama dipercaya, Anda dapat mempertimbangkan untuk menentukan rangkaian algoritme tanpa tanda tangan digital. Namun, kami sangat merekomendasikan rangkaian algoritme yang mencakup komitmen kunci dan fungsi derivasi kunci. Suite algoritma tanpa fitur ini hanya didukung untuk kompatibilitas mundur.

Manajer materi kriptografi

Manajer bahan kriptografi (CMM) merakit bahan kriptografi yang digunakan untuk mengenkripsi dan mendekripsi data. Materi kriptografi termasuk plaintext dan kunci data terenkripsi, dan kunci penandatanganan pesan opsional. Anda tidak pernah berinteraksi dengan CMM secara langsung. Metode enkripsi dan dekripsi menanganinya untuk Anda.

Anda dapat menggunakan CMM default atau CMM caching yang AWS Encryption SDK disediakan, atau menulis CMM kustom. Dan Anda dapat menentukan CMM, tetapi itu tidak diperlukan. Saat Anda menentukan keyring atau penyedia kunci master, CMM AWS Encryption SDK default akan dibuat untuk Anda. CMM default mendapatkan materi enkripsi atau dekripsi dari keyring atau penyedia kunci utama yang Anda tentukan. Ini mungkin melibatkan panggilan ke layanan kriptografi, seperti AWS Key Management Service(AWS KMS).

Karena CMM bertindak sebagai penghubung antara keyring AWS Encryption SDK dan keyring (atau penyedia kunci utama), ini adalah titik ideal untuk penyesuaian dan ekstensi, seperti dukungan untuk penegakan kebijakan dan caching. AWS Encryption SDK Ini menyediakan CMM caching untuk mendukung caching kunci data.

Enkripsi simetris dan asimetris

Enkripsi simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

Enkripsi asimetris menggunakan data key pair yang terkait secara matematis. Satu kunci dalam pasangan mengenkripsi data; hanya kunci lain dalam pasangan yang dapat mendekripsi data.

AWS Encryption SDK Menggunakan enkripsi amplop. Ini mengenkripsi data Anda dengan kunci data simetris. Ini mengenkripsi kunci data simetris dengan satu atau lebih tombol pembungkus simetris atau asimetris. Ia mengembalikan pesan terenkripsi yang mencakup data terenkripsi dan setidaknya satu salinan kunci data terenkripsi.

Mengenkripsi data Anda (enkripsi simetris)

Untuk mengenkripsi data Anda, AWS Encryption SDK menggunakan kunci data simetris dan rangkaian algoritma yang menyertakan algoritma enkripsi simetris. Untuk mendekripsi data, AWS Encryption SDK menggunakan kunci data yang sama dan rangkaian algoritma yang sama.

Mengenkripsi kunci data Anda (enkripsi simetris atau asimetris)

Penyedia keyring atau kunci utama yang Anda berikan ke operasi enkripsi dan dekripsi menentukan bagaimana kunci data simetris dienkripsi dan didekripsi. Anda dapat memilih keyring atau penyedia kunci utama yang menggunakan enkripsi simetris, seperti AWS KMS keyring, atau yang menggunakan enkripsi asimetris, seperti keyring RSA mentah atau. `JceMasterKey`

Komitmen utama

AWS Encryption SDK Mendukung komitmen kunci (kadang-kadang dikenal sebagai ketahanan), properti keamanan yang menjamin bahwa setiap ciphertext dapat didekripsi hanya untuk satu plaintext. Untuk melakukan ini, komitmen utama menjamin bahwa hanya kunci data yang mengenkripsi pesan Anda yang akan digunakan untuk mendekripsi itu. Mengenkripsi dan mendekripsi dengan komitmen utama adalah praktik terbaik.AWS Encryption SDK

Sebagian besar cipher simetris modern (termasuk AES) mengenkripsi plaintext di bawah satu kunci rahasia, seperti kunci data unik yang digunakan untuk mengenkripsi setiap pesan teks biasa. AWS Encryption SDK Mendekripsi data ini dengan kunci data yang sama mengembalikan plaintext yang identik dengan aslinya. Mendekripsi dengan kunci yang berbeda biasanya akan gagal. Namun, dimungkinkan untuk mendekripsi ciphertext di bawah dua kunci yang berbeda. Dalam kasus yang jarang terjadi, adalah layak untuk menemukan kunci yang dapat mendekripsi beberapa byte ciphertext menjadi plaintext yang berbeda, tetapi masih dapat dipahami.

AWS Encryption SDK Selalu mengenkripsi setiap pesan teks biasa di bawah satu kunci data unik. Mungkin mengenkripsi kunci data itu di bawah beberapa kunci pembungkus (atau kunci master), tetapi kunci pembungkus selalu mengenkripsi kunci data yang sama. Meskipun demikian, pesan terenkripsi yang canggih dan dibuat secara manual mungkin sebenarnya berisi kunci data yang berbeda, masing-masing dienkripsi oleh kunci pembungkus yang berbeda. Misalnya, jika satu

pengguna mendekripsi pesan terenkripsi, ia mengembalikan 0x0 (false) sementara pengguna lain yang mendekripsi pesan terenkripsi yang sama mendapat 0x1 (true).

Untuk mencegah skenario ini, AWS Encryption SDK mendukung komitmen utama saat mengenkripsi dan mendekripsi. Ketika AWS Encryption SDK mengenkripsi pesan dengan komitmen utama, secara kriptografis mengikat kunci data unik yang menghasilkan ciphertext ke string komitmen kunci, pengidentifikasi kunci data non-rahasia. Kemudian menyimpan string komitmen utama dalam metadata pesan terenkripsi. Ketika mendekripsi pesan dengan komitmen utama, AWS Encryption SDK memverifikasi bahwa kunci data adalah satu-satunya kunci untuk pesan terenkripsi itu. Jika verifikasi kunci data gagal, operasi dekripsi gagal.

Support untuk komitmen utama diperkenalkan di versi 1.7. x, yang dapat mendekripsi pesan dengan komitmen utama, tetapi tidak akan mengenkripsi dengan komitmen utama. Anda dapat menggunakan versi ini untuk sepenuhnya menyebarkan kemampuan untuk mendekripsi ciphertext dengan komitmen utama. Versi 2.0. x mencakup dukungan penuh untuk komitmen utama. Secara default, ini mengenkripsi dan mendekripsi hanya dengan komitmen utama. Ini adalah konfigurasi yang ideal untuk aplikasi yang tidak perlu mendekripsi ciphertext yang dienkripsi oleh versi sebelumnya. AWS Encryption SDK

Meskipun mengenkripsi dan mendekripsi dengan komitmen utama adalah praktik terbaik, kami membiarkan Anda memutuskan kapan itu digunakan, dan membiarkan Anda menyesuaikan kecepatan Anda mengadopsinya. Dimulai pada versi 1.7. x, AWS Encryption SDK mendukung kebijakan komitmen yang menetapkan rangkaian algoritme default dan membatasi rangkaian algoritme yang dapat digunakan. Kebijakan ini menentukan apakah data Anda dienkripsi dan didekripsi dengan komitmen utama.

Komitmen utama menghasilkan pesan terenkripsi yang sedikit lebih besar (+ 30 byte) dan membutuhkan lebih banyak waktu untuk diproses. Jika aplikasi Anda sangat sensitif terhadap ukuran atau kinerja, Anda dapat memilih untuk keluar dari komitmen utama. Tetapi lakukan hanya jika Anda harus.

Untuk informasi selengkapnya tentang migrasi ke versi 1.7. x dan 2.0. x, termasuk fitur komitmen utama mereka, lihatMigrasi Anda AWS Encryption SDK. Untuk informasi teknis tentang komitmen utama, lihat the section called “Referensi algoritma” danthe section called “Referensi format pesan”.

Kebijakan komitmen

Kebijakan komitmen adalah pengaturan konfigurasi yang menentukan apakah aplikasi Anda mengenkripsi dan mendekripsi dengan komitmen utama. Mengenkripsi dan mendekripsi dengan komitmen utama adalah praktik terbaik.AWS Encryption SDK

Kebijakan komitmen memiliki tiga nilai.

> **Note**
>
> Anda mungkin harus menggulir secara horizontal atau vertikal untuk melihat seluruh tabel.

Nilai-nilai kebijakan komitmen

Nilai	Enkripsi dengan komitmen utama	Enkripsi tanpa komitmen utama	Dekripsi dengan komitmen utama	Mendekripsi tanpa komitmen utama
ForbidEncryptAllowDecrypt	✗	✓	✓	✓
RequireEncryptAllowDecrypt	✓	✗	✓	✓
RequireEncryptRequireDecrypt	✓	✗	✓	✗

Pengaturan kebijakan komitmen diperkenalkan di AWS Encryption SDK versi 1.7. x. Ini berlaku di semua bahasa pemrograman yang didukung.

- `ForbidEncryptAllowDecrypt`mendekripsi dengan atau tanpa komitmen utama, tetapi tidak akan mengenkripsi dengan komitmen utama. Nilai ini, diperkenalkan dalam versi 1.7. x, dirancang untuk mempersiapkan semua host yang menjalankan aplikasi Anda untuk mendekripsi dengan komitmen utama sebelum mereka menemukan ciphertext yang dienkripsi dengan komitmen utama.

- `RequireEncryptAllowDecrypt`selalu mengenkripsi dengan komitmen utama. Itu dapat mendekripsi dengan atau tanpa komitmen utama. Nilai ini, diperkenalkan dalam versi 2.0. x, memungkinkan Anda mulai mengenkripsi dengan komitmen utama, tetapi masih mendekripsi ciphertext lama tanpa komitmen utama.
- `RequireEncryptRequireDecrypt`mengenkripsi dan mendekripsi hanya dengan komitmen utama. Nilai ini adalah default untuk versi 2.0. x. Gunakan nilai ini ketika Anda yakin bahwa semua ciphertext Anda dienkripsi dengan komitmen utama.

Pengaturan kebijakan komitmen menentukan rangkaian algoritme mana yang dapat Anda gunakan. Dimulai pada versi 1.7. x, AWS Encryption SDK mendukung rangkaian algoritma untuk komitmen utama; dengan dan tanpa penandatanganan. Jika Anda menentukan rangkaian algoritme yang bertentangan dengan kebijakan komitmen Anda, AWS Encryption SDK kesalahan akan ditampilkan.

Untuk bantuan menetapkan kebijakan komitmen Anda, lihatMenetapkan kebijakan komitmen Anda.

Tanda tangan digital

AWS Encryption SDK Enkripsi data Anda menggunakan algoritma enkripsi yang diautentikasi, AES-GCM, dan proses dekripsi memverifikasi integritas dan keaslian pesan terenkripsi tanpa menggunakan tanda tangan digital. Tetapi karena AES-GCM menggunakan kunci simetris, siapa pun yang dapat mendekripsi kunci data yang digunakan untuk mendekripsi ciphertext juga dapat secara manual membuat ciphertext terenkripsi baru, yang menyebabkan masalah keamanan potensial. Misalnya, jika Anda menggunakan AWS KMS key sebagai kunci pembungkus, pengguna dengan `kms:Decrypt` izin dapat membuat ciphertext terenkripsi tanpa menelepon. `kms:Encrypt`

Untuk menghindari masalah ini, AWS Encryption SDK dukungan menambahkan tanda tangan Elliptic Curve Digital Signature Algorithm (ECDSA) ke akhir pesan terenkripsi. Ketika rangkaian algoritma penandatanganan digunakan, akan AWS Encryption SDK menghasilkan kunci pribadi sementara dan public key pair untuk setiap pesan terenkripsi. AWS Encryption SDK Menyimpan kunci publik dalam konteks enkripsi kunci data dan membuang kunci pribadi. Ini memastikan bahwa tidak ada yang dapat membuat tanda tangan lain yang memverifikasi dengan kunci publik. Algoritma mengikat kunci publik ke kunci data terenkripsi sebagai data otentikasi tambahan di header pesan, mencegah pengguna yang hanya dapat mendekripsi pesan dari mengubah kunci publik atau memengaruhi verifikasi tanda tangan.

Verifikasi tanda tangan menambahkan biaya kinerja yang signifikan pada dekripsi. Jika pengguna mengenkripsi data dan pengguna yang mendekripsi data sama-sama dipercaya, pertimbangkan untuk menggunakan rangkaian algoritme yang tidak menyertakan penandatanganan.

> **Note**
>
> Jika keyring atau akses ke materi kriptografi pembungkus tidak menggambarkan antara enkripsi dan dekripsi, tanda tangan digital tidak memberikan nilai kriptografi.

AWS KMS keyrings, termasuk AWS KMS keyring RSA asimetris, dapat menggambarkan antara enkripsi dan dekripsi berdasarkan kebijakan utama dan kebijakan IAM. AWS KMS

Karena sifat kriptografinya, gantungan kunci berikut tidak dapat menggambarkan antara enkripsi dan dekripsi:

- AWS KMS Gantungan kunci hierarkis
- AWS KMS Gantungan kunci ECDH
- Gantungan kunci AES mentah
- Gantungan kunci RSA mentah
- Gantungan kunci ECDH mentah

Bagaimana cara AWS Encryption SDK kerjanya

Alur kerja di bagian ini menjelaskan cara AWS Encryption SDK mengenkripsi data dan mendekripsi pesan terenkripsi. Alur kerja ini menjelaskan proses dasar menggunakan fitur default. Untuk detail tentang mendefinisikan dan menggunakan komponen kustom, lihat GitHub repositori untuk setiap implementasi bahasa yang didukung.

AWS Encryption SDK Menggunakan enkripsi amplop untuk melindungi data Anda. Setiap pesan dienkripsi di bawah kunci data unik. Kemudian kunci data dienkripsi oleh kunci pembungkus yang Anda tentukan. Untuk mendekripsi pesan terenkripsi, AWS Encryption SDK menggunakan kunci pembungkus yang Anda tentukan untuk mendekripsi setidaknya satu kunci data terenkripsi. Kemudian dapat mendekripsi ciphertext dan mengembalikan pesan teks biasa.

Butuh bantuan dengan terminologi yang kita gunakan di? AWS Encryption SDK Lihat the section called “Konsep”.

Bagaimana AWS Encryption SDK mengenkripsi data

AWS Encryption SDK Ini menyediakan metode yang mengenkripsi string, array byte, dan aliran byte. Untuk contoh kode, lihat topik Contoh di setiap Bahasa pemrograman bagian.

1. Buat keyring (atau penyedia kunci utama) yang menentukan kunci pembungkus yang melindungi data Anda.
2. Teruskan data keyring dan plaintext ke metode enkripsi. Kami menyarankan Anda meneruskan konteks enkripsi opsional dan non-rahasia.
3. Metode enkripsi meminta keyring untuk bahan enkripsi. Keyring mengembalikan kunci enkripsi data unik untuk pesan: satu kunci data teks biasa dan satu salinan kunci data yang dienkripsi oleh masing-masing kunci pembungkus yang ditentukan.
4. Metode enkripsi menggunakan kunci data plaintext untuk mengenkripsi data, dan kemudian membuang kunci data plaintext. Jika Anda menyediakan konteks enkripsi (praktik AWS Encryption SDK terbaik), metode enkripsi secara kriptografis mengikat konteks enkripsi ke data terenkripsi.
5. Metode enkripsi mengembalikan pesan terenkripsi yang berisi data terenkripsi, kunci data terenkripsi, dan metadata lainnya, termasuk konteks enkripsi, jika Anda menggunakannya.

Bagaimana AWS Encryption SDK mendekripsi pesan terenkripsi

AWS Encryption SDK Menyediakan metode yang mendekripsi pesan terenkripsi dan mengembalikan plaintext. Untuk contoh kode, lihat topik Contoh di setiap Bahasa pemrograman bagian.

Keyring (atau penyedia kunci utama) yang mendekripsi pesan terenkripsi harus kompatibel dengan yang digunakan untuk mengenkripsi pesan. Salah satu kunci pembungkusnya harus dapat mendekripsi kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi tentang kompatibilitas dengan keyrings dan penyedia kunci utama, lihatthe section called “Kompatibilitas keyring”.

1. Buat keyring atau penyedia kunci master dengan kunci pembungkus yang dapat mendekripsi data Anda. Anda dapat menggunakan keyring yang sama dengan yang Anda berikan ke metode enkripsi atau yang berbeda.
2. Teruskan pesan terenkripsi dan keyring ke metode dekripsi.
3. Metode dekripsi meminta keyring atau penyedia kunci master untuk mendekripsi salah satu kunci data terenkripsi dalam pesan terenkripsi. Ini meneruskan informasi dari pesan terenkripsi, termasuk kunci data terenkripsi.
4. Keyring menggunakan kunci pembungkusnya untuk mendekripsi salah satu kunci data terenkripsi. Jika berhasil, responsnya menyertakan kunci data plaintext. Jika tidak ada kunci pembungkus yang ditentukan oleh keyring atau penyedia kunci master dapat mendekripsi kunci data terenkripsi, panggilan dekripsi gagal.

5. Metode dekripsi menggunakan kunci data plaintext untuk mendekripsi data, membuang kunci data plaintext, dan mengembalikan data plaintext.

Suite algoritma yang didukung di AWS Encryption SDK

Sebuah algoritma suite adalah kumpulan algoritma kriptografi dan nilai-nilai terkait. Sistem kriptografi menggunakan implementasi algoritma untuk menghasilkan pesan ciphertext.

Rangkaian AWS Encryption SDK algoritma menggunakan algoritma Advanced Encryption Standard (AES) dalam Galois/Counter Mode (GCM), yang dikenal sebagai AES-GCM, untuk mengenkripsi data mentah. AWS Encryption SDK Mendukung kunci enkripsi 256-bit, 192-bit, dan 128-bit. Panjang vektor inisialisasi (IV) selalu 12 byte. Panjang tag otentikasi selalu 16 byte.

Secara default, AWS Encryption SDK menggunakan rangkaian algoritma dengan AES-GCM dengan fungsi derivasi extract-and-expand kunci berbasis HMAC (HKDF), penandatanganan, dan kunci enkripsi 256-bit. Jika kebijakan komitmen memerlukan komitmen utama, AWS Encryption SDK memilih rangkaian algoritme yang juga mendukung komitmen utama; jika tidak, ia memilih rangkaian algoritme dengan derivasi dan penandatanganan kunci, tetapi bukan komitmen utama.

Direkomendasikan: AES-GCM dengan derivasi kunci, penandatanganan, dan komitmen utama

Ini AWS Encryption SDK merekomendasikan rangkaian algoritma yang memperoleh kunci enkripsi AES-GCM dengan memasok kunci enkripsi data 256-bit ke fungsi derivasi kunci berbasis HMAC (extract-and-expandHKDF). AWS Encryption SDK Menambahkan tanda tangan Elliptic Curve Digital Signature Algorithm (ECDSA). Untuk mendukung komitmen utama, rangkaian algoritme ini juga memperoleh string komitmen utama — pengidentifikasi kunci data non-rahasia — yang disimpan dalam metadata pesan terenkripsi. String komitmen kunci ini juga diturunkan melalui HKDF menggunakan prosedur yang mirip dengan menurunkan kunci enkripsi data.

AWS Encryption SDK Suite Algoritma

Enkripsi algoritme	Panjang kunci enkripsi data (dalam bit)	Algoritma derivasi kunci	Algoritma tanda tangan	Komitmen utama
AES-GCM	256	HKDF dengan SHA-384	ECDSA dengan P-384 dan SHA-384	HKDF dengan SHA-512

HKDF membantu Anda menghindari penggunaan kembali kunci enkripsi data yang tidak disengaja dan mengurangi risiko penggunaan kunci data secara berlebihan.

Untuk penandatanganan, rangkaian algoritma ini menggunakan ECDSA dengan algoritma fungsi hash kriptografi (SHA-384). ECDSA digunakan secara default, meskipun tidak ditentukan oleh kebijakan untuk kunci master yang mendasarinya. Penandatanganan pesan memverifikasi bahwa pengirim pesan diberi wewenang untuk mengenkripsi pesan dan memberikan non-penolakan. Hal ini sangat berguna ketika kebijakan otorisasi untuk kunci master memungkinkan satu set pengguna untuk mengenkripsi data dan satu set pengguna yang berbeda untuk mendekripsi data.

Rangkaian algoritma dengan komitmen utama memastikan bahwa setiap ciphertext mendekripsi hanya satu teks biasa. Mereka melakukan ini dengan memvalidasi identitas kunci data yang digunakan sebagai input ke algoritma enkripsi. Saat mengenkripsi, rangkaian algoritma ini memperoleh string komitmen utama. Sebelum mendekripsi, mereka memvalidasi bahwa kunci data cocok dengan string komitmen kunci. Jika tidak, panggilan dekripsi gagal.

Suite algoritma lain yang didukung

AWS Encryption SDK Mendukung rangkaian algoritma alternatif berikut untuk kompatibilitas mundur. Secara umum, kami tidak merekomendasikan suite algoritma ini. Namun, kami menyadari bahwa penandatanganan dapat menghambat kinerja secara signifikan, jadi kami menawarkan rangkaian komitmen utama dengan derivasi kunci untuk kasus-kasus tersebut. Untuk aplikasi yang harus membuat pengorbanan kinerja yang lebih signifikan, kami terus menawarkan suite yang tidak memiliki penandatanganan, komitmen utama, dan derivasi kunci.

AES-GCM tanpa komitmen utama

Suite algoritma tanpa komitmen kunci tidak memvalidasi kunci data sebelum mendekripsi. Akibatnya, rangkaian algoritma ini dapat mendekripsi satu ciphertext menjadi pesan teks biasa

yang berbeda. Namun, karena rangkaian algoritma dengan komitmen utama menghasilkan pesan terenkripsi yang sedikit lebih besar (+30 byte) dan membutuhkan waktu lebih lama untuk diproses, mereka mungkin bukan pilihan terbaik untuk setiap aplikasi.

Ini AWS Encryption SDK mendukung rangkaian algoritme dengan derivasi kunci, komitmen utama, penandatanganan, dan satu dengan derivasi kunci dan komitmen utama, tetapi tidak menandatangani. Kami tidak menyarankan menggunakan rangkaian algoritma tanpa komitmen utama. Jika Anda harus, kami merekomendasikan rangkaian algoritme dengan derivasi kunci dan komitmen kunci, tetapi tidak menandatangani. Namun, jika profil kinerja aplikasi Anda mendukung penggunaan rangkaian algoritme, menggunakan rangkaian algoritme dengan komitmen utama, derivasi kunci, dan penandatanganan adalah praktik terbaik.

AES-GCM tanpa penandatanganan

Suite algoritma tanpa penandatanganan tidak memiliki tanda tangan ECDSA yang memberikan keaslian dan non-penolakan. Gunakan suite ini hanya ketika pengguna yang mengenkripsi data dan mereka yang mendekripsi data sama-sama dipercaya.

Saat menggunakan rangkaian algoritme tanpa penandatanganan, kami sarankan Anda memilih satu dengan derivasi kunci dan komitmen kunci.

AES-GCM tanpa derivasi kunci

Suite algoritma tanpa derivasi kunci menggunakan kunci enkripsi data sebagai kunci enkripsi AES-GCM, alih-alih menggunakan fungsi derivasi kunci untuk mendapatkan kunci unik. Kami tidak menyarankan menggunakan suite ini untuk menghasilkan ciphertext, tetapi AWS Encryption SDK mendukungnya untuk alasan kompatibilitas.

Untuk informasi lebih lanjut tentang bagaimana suite ini diwakili dan digunakan di perpustakaan, lihatthe section called “Referensi algoritma”.

Menggunakan AWS Encryption SDK dengan AWS KMS

Untuk menggunakan AWS Encryption SDK, Anda perlu mengkonfigurasi keyrings atau penyedia kunci master dengan kunci pembungkus. Jika Anda tidak memiliki infrastruktur utama, sebaiknya gunakan AWS Key Management Service (AWS KMS). Banyak contoh kode di AWS Encryption SDK require an AWS KMS key.

Untuk berinteraksi AWS KMS, AWS Encryption SDK diperlukan AWS SDK untuk bahasa pemrograman pilihan Anda. Pustaka AWS Encryption SDK klien bekerja dengan AWS SDKs untuk mendukung kunci master yang disimpan di AWS KMS.

Untuk mempersiapkan untuk menggunakan AWS Encryption SDK dengan AWS KMS

1. Buat sebuah Akun AWS. Untuk mempelajari caranya, lihat Bagaimana cara membuat dan mengaktifkan akun Amazon Web Services baru? di pusat AWS pengetahuan.
2. Buat enkripsi AWS KMS key simetris. Untuk bantuan, lihat Membuat Kunci di Panduan AWS Key Management Service Pengembang.

   > **Tip**
   >
   > Untuk menggunakan AWS KMS key pemrograman, Anda akan memerlukan ID kunci atau Nama Sumber Daya Amazon (ARN) dari file. AWS KMS keyUntuk bantuan menemukan ID atau ARN AWS KMS key, lihat Menemukan ID Kunci dan ARN di Panduan Pengembang.AWS Key Management Service

3. Hasilkan ID kunci akses dan kunci akses keamanan. Anda dapat menggunakan ID kunci akses dan kunci akses rahasia untuk pengguna IAM atau Anda dapat menggunakan AWS Security Token Service untuk membuat sesi baru dengan kredenal keamanan sementara yang mencakup ID kunci akses, kunci akses rahasia, dan token sesi. Sebagai praktik keamanan terbaik, kami menyarankan Anda menggunakan kredenal sementara alih-alih kredensi jangka panjang yang terkait dengan pengguna IAM atau akun pengguna AWS (root) Anda.

   Untuk membuat pengguna IAM dengan kunci akses, lihat Membuat Pengguna IAM di Panduan Pengguna IAM.

   Untuk menghasilkan kredenal keamanan sementara, lihat Meminta kredenal keamanan sementara di Panduan Pengguna IAM.

4. Tetapkan AWS kredensi Anda menggunakan instruksi di AWS SDK for Java, AWS SDK for JavaScript, AWS SDK untuk Python (Boto)atau AWS SDK untuk C++(untuk C), dan ID kunci akses dan kunci akses rahasia yang Anda buat di langkah 3. Jika Anda membuat kredensi sementara, Anda juga perlu menentukan token sesi.

   Prosedur ini memungkinkan AWS SDKs untuk menandatangani permintaan AWS untuk Anda. Contoh kode dalam AWS Encryption SDK yang berinteraksi dengan AWS KMS berasumsi bahwa Anda telah menyelesaikan langkah ini.
5. Unduh dan instal AWS Encryption SDK. Untuk mempelajari caranya, lihat petunjuk penginstalan untuk bahasa pemrograman yang ingin Anda gunakan.

Praktik terbaik untuk AWS Encryption SDK

AWS Encryption SDK Ini dirancang untuk memudahkan Anda melindungi data Anda menggunakan standar industri dan praktik terbaik. Meskipun banyak praktik terbaik dipilih untuk Anda dalam nilai default, beberapa praktik bersifat opsional tetapi disarankan kapan pun praktis.

Gunakan versi terbaru

Saat Anda mulai menggunakan AWS Encryption SDK, gunakan versi terbaru yang ditawarkan dalam bahasa pemrograman pilihan Anda. Jika Anda telah menggunakan AWS Encryption SDK, tingkatkan ke setiap versi terbaru sesegera mungkin. Ini memastikan bahwa Anda menggunakan konfigurasi yang disarankan dan memanfaatkan properti keamanan baru untuk melindungi data Anda. Untuk detail tentang versi yang didukung, termasuk panduan untuk migrasi dan penerapan, lihat Support dan pemeliharaan danVersi dari AWS Encryption SDK.

Jika versi baru menghentikan elemen dalam kode Anda, ganti mereka sesegera mungkin. Peringatan penghentian dan komentar kode biasanya merekomendasikan alternatif yang baik.

Untuk membuat peningkatan signifikan lebih mudah dan tidak rentan terhadap kesalahan, kami sesekali menyediakan rilis sementara atau transisi. Gunakan rilis ini, dan dokumentasi yang menyertainya, untuk memastikan bahwa Anda dapat meningkatkan aplikasi tanpa mengganggu alur kerja produksi Anda.

Gunakan nilai default

AWS Encryption SDK Desain praktik terbaik ke dalam nilai defaultnya. Kapan pun memungkinkan, gunakan mereka. Untuk kasus di mana default tidak praktis, kami menyediakan alternatif, seperti rangkaian algoritma tanpa penandatanganan. Kami juga memberikan kesempatan kepada pengguna tingkat lanjut untuk kustomisasi, seperti gantungan kunci khusus, penyedia kunci utama, dan manajer materi kriptografi ()CMMs. Gunakan alternatif canggih ini dengan hati-hati dan mintalah pilihan Anda diverifikasi oleh insinyur keamanan bila memungkinkan.

Gunakan konteks enkripsi

Untuk meningkatkan keamanan operasi kriptografi Anda, sertakan konteks enkripsi dengan nilai yang berarti dalam semua permintaan untuk mengenkripsi data. Menggunakan konteks enkripsi adalah opsional, tetapi ini adalah praktik terbaik kriptografi yang kami rekomendasikan. Konteks enkripsi menyediakan data otentikasi tambahan (AAD) untuk enkripsi yang diautentikasi di file. AWS Encryption SDK Meskipun bukan rahasia, konteks enkripsi dapat membantu Anda melindungi integritas dan keaslian data terenkripsi Anda.

Dalam AWS Encryption SDK, Anda menentukan konteks enkripsi hanya saat mengenkripsi. Saat mendekripsi, AWS Encryption SDK menggunakan konteks enkripsi di header pesan terenkripsi yang dikembalikan. AWS Encryption SDK Sebelum aplikasi Anda mengembalikan data teks biasa, verifikasi bahwa konteks enkripsi yang Anda gunakan untuk mengenkripsi pesan disertakan dalam konteks enkripsi yang digunakan untuk mendekripsi pesan. Untuk detailnya, lihat contoh dalam bahasa pemrograman Anda.

Saat Anda menggunakan antarmuka baris perintah, AWS Encryption SDK memverifikasi konteks enkripsi untuk Anda.

Lindungi kunci pembungkus Anda

Ini AWS Encryption SDK menghasilkan kunci data unik untuk mengenkripsi setiap pesan teks biasa. Kemudian mengenkripsi kunci data dengan kunci pembungkus yang Anda berikan. Jika kunci pembungkus Anda hilang atau dihapus, data terenkripsi Anda tidak dapat dipulihkan. Jika kunci Anda tidak diamankan, data Anda mungkin rentan.

Gunakan kunci pembungkus yang dilindungi oleh infrastruktur kunci aman, seperti AWS Key Management Service(AWS KMS). Saat menggunakan kunci AES mentah atau RSA mentah, gunakan sumber keacakan dan penyimpanan tahan lama yang memenuhi persyaratan keamanan Anda. Membuat dan menyimpan kunci pembungkus dalam modul keamanan perangkat keras (HSM), atau layanan yang menyediakan HSMs, seperti AWS CloudHSM, adalah praktik terbaik.

Gunakan mekanisme otorisasi infrastruktur kunci Anda untuk membatasi akses ke kunci pembungkus Anda hanya untuk pengguna yang membutuhkannya. Menerapkan prinsip-prinsip praktik terbaik, seperti hak istimewa paling sedikit. Saat menggunakan AWS KMS keys, gunakan kebijakan utama dan kebijakan IAM yang menerapkan prinsip-prinsip praktik terbaik.

Tentukan kunci pembungkus Anda

Itu selalu merupakan praktik terbaik untuk menentukan kunci pembungkus Anda secara eksplisit saat mendekripsi, serta mengenkripsi. Ketika Anda melakukannya, hanya AWS Encryption SDK menggunakan kunci yang Anda tentukan. Praktik ini memastikan bahwa Anda hanya menggunakan kunci enkripsi yang Anda inginkan. Untuk AWS KMS membungkus kunci, ini juga meningkatkan kinerja dengan mencegah Anda menggunakan kunci secara tidak sengaja di wilayah Akun AWS atau yang berbeda, atau mencoba mendekripsi dengan kunci yang tidak memiliki izin untuk digunakan.

Saat mengenkripsi, gantungan kunci dan penyedia kunci utama yang diperlukan AWS Encryption SDK persediaan agar Anda menentukan kunci pembungkus. Mereka menggunakan semua dan hanya kunci pembungkus yang Anda tentukan. Anda juga diminta untuk menentukan

kunci pembungkus saat mengenkripsi dan mendekripsi dengan gantungan kunci AES mentah, gantungan kunci RSA mentah, dan Kunci. JCEMaster

Namun, saat mendekripsi dengan AWS KMS keyrings dan penyedia kunci master, Anda tidak diharuskan menentukan kunci pembungkus. AWS Encryption SDK Bisa mendapatkan pengenal kunci dari metadata kunci data terenkripsi. Tetapi menentukan kunci pembungkus adalah praktik terbaik yang kami rekomendasikan.

Untuk mendukung praktik terbaik ini saat bekerja dengan kunci AWS KMS pembungkus, kami merekomendasikan hal berikut:

- Gunakan AWS KMS keyrings yang menentukan tombol pembungkus. Saat mengenkripsi dan mendekripsi, gantungan kunci ini hanya menggunakan kunci pembungkus tertentu yang Anda tentukan.
- Saat menggunakan kunci AWS KMS master dan penyedia kunci master, gunakan konstruktor mode ketat yang diperkenalkan di versi 1.7. x dari AWS Encryption SDK. Mereka membuat penyedia yang mengenkripsi dan mendekripsi hanya dengan kunci pembungkus yang Anda tentukan. Konstruktor untuk penyedia kunci master yang selalu mendekripsi dengan kunci pembungkus apa pun tidak digunakan lagi di versi 1.7. x dan dihapus dalam versi 2.0. x.

Saat menentukan kunci AWS KMS pembungkus untuk mendekripsi tidak praktis, Anda dapat menggunakan penyedia penemuan. AWS Encryption SDK Di C dan JavaScript mendukung keyrings AWS KMS penemuan. Penyedia kunci master dengan mode penemuan tersedia untuk Java dan Python dalam versi 1.7. x dan kemudian. Penyedia penemuan ini, yang hanya digunakan untuk mendekripsi dengan kunci AWS KMS pembungkus, secara eksplisit mengarahkan AWS Encryption SDK untuk menggunakan kunci pembungkus apa pun yang mengenkripsi kunci data.

Jika Anda harus menggunakan penyedia penemuan, gunakan fitur filter penemuannya untuk membatasi kunci pembungkus yang mereka gunakan. Misalnya, keyring penemuan AWS KMS regional hanya menggunakan kunci pembungkus tertentu. Wilayah AWS Anda juga dapat mengonfigurasi AWS KMS keyrings dan penyedia kunci AWS KMS master untuk hanya menggunakan kunci pembungkus pada khususnya. Akun AWS Juga, seperti biasa, gunakan kebijakan utama dan kebijakan IAM untuk mengontrol akses ke kunci AWS KMS pembungkus Anda.

Gunakan tanda tangan digital

Ini adalah praktik terbaik untuk menggunakan rangkaian algoritma dengan penandatanganan. Tanda tangan digital memverifikasi bahwa pengirim pesan diberi wewenang untuk mengirim

pesan dan melindungi integritas pesan. Semua versi suite algoritma AWS Encryption SDK penggunaan dengan penandatanganan secara default.

Jika persyaratan keamanan Anda tidak menyertakan tanda tangan digital, Anda dapat memilih rangkaian algoritme tanpa tanda tangan digital. Namun, kami merekomendasikan penggunaan tanda tangan digital, terutama ketika satu kelompok pengguna mengenkripsi data dan kumpulan pengguna yang berbeda mendekripsi data tersebut.

Gunakan komitmen utama

Ini adalah praktik terbaik untuk menggunakan fitur keamanan komitmen utama. Dengan memverifikasi identitas kunci data unik yang mengenkripsi data Anda, komitmen kunci mencegah Anda mendekripsi ciphertext apa pun yang dapat menghasilkan lebih dari satu pesan teks biasa.

AWS Encryption SDK Ini memberikan dukungan penuh untuk mengenkripsi dan mendekripsi dengan komitmen utama yang dimulai pada versi 2.0. x. Secara default, semua pesan Anda dienkripsi dan didekripsi dengan komitmen utama. Versi 1.7. x dari AWS Encryption SDK kaleng mendekripsi ciphertext dengan komitmen utama. Ini dirancang untuk membantu pengguna versi sebelumnya menyebarkan versi 2.0. x berhasil.

Support for key commitment mencakup rangkaian algoritma baru dan format pesan baru yang menghasilkan ciphertext hanya 30 byte lebih besar dari ciphertext tanpa komitmen kunci. Desain meminimalkan dampaknya pada kinerja sehingga sebagian besar pengguna dapat menikmati manfaat dari komitmen utama. Jika aplikasi Anda sangat sensitif terhadap ukuran dan kinerja, Anda dapat memutuskan untuk menggunakan pengaturan kebijakan komitmen untuk menonaktifkan komitmen utama atau mengizinkan AWS Encryption SDK untuk mendekripsi pesan tanpa komitmen, tetapi melakukannya hanya jika Anda harus.

Batasi jumlah kunci data terenkripsi

Ini adalah praktik terbaik untuk membatasi jumlah kunci data terenkripsi dalam pesan yang Anda dekripsi, terutama pesan dari sumber yang tidak tepercaya. Mendekripsi pesan dengan banyak kunci data terenkripsi yang tidak dapat Anda dekripsi dapat menyebabkan penundaan yang diperpanjang, menghabiskan biaya, membatasi aplikasi Anda dan orang lain yang berbagi akun Anda, dan berpotensi menghabiskan infrastruktur utama Anda. Tanpa batas, pesan terenkripsi dapat memiliki hingga 65.535 (2^16 - 1) kunci data terenkripsi. Lihat perinciannya di Membatasi kunci data terenkripsi.

Untuk informasi selengkapnya tentang fitur AWS Encryption SDK keamanan yang mendasari praktik terbaik ini, lihat Peningkatan enkripsi sisi klien: Komitmen eksplisit KeyIds dan kunci di Blog Keamanan.AWS

Mengkonfigurasi AWS Encryption SDK

AWS Encryption SDK Ini dirancang agar mudah digunakan. Meskipun AWS Encryption SDK memiliki beberapa opsi konfigurasi, nilai default dipilih dengan cermat agar praktis dan aman untuk sebagian besar aplikasi. Namun, Anda mungkin perlu menyesuaikan konfigurasi untuk meningkatkan kinerja atau menyertakan fitur khusus dalam desain Anda.

Saat mengonfigurasi implementasi Anda, tinjau praktik AWS Encryption SDK terbaik dan terapkan sebanyak yang Anda bisa.

Topik

Memilih bahasa pemrograman

AWS Encryption SDK Ini tersedia dalam berbagai bahasa pemrograman. Implementasi bahasa dirancang untuk sepenuhnya dapat dioperasikan dan menawarkan fitur yang sama, meskipun mereka mungkin diimplementasikan dengan cara yang berbeda. Biasanya, Anda menggunakan perpustakaan yang kompatibel dengan aplikasi Anda. Namun, Anda dapat memilih bahasa pemrograman untuk implementasi tertentu. Misalnya, jika Anda lebih suka bekerja dengan gantungan kunci, Anda dapat memilih AWS Encryption SDK for C atau. AWS Encryption SDK for JavaScript

Memilih tombol pembungkus

Ini AWS Encryption SDK menghasilkan kunci data simetris yang unik untuk mengenkripsi setiap pesan. Kecuali Anda menggunakan caching kunci data, Anda tidak perlu mengkonfigurasi, mengelola, atau menggunakan kunci data. Yang AWS Encryption SDK melakukannya untuk Anda.

Namun, Anda harus memilih satu atau lebih kunci pembungkus untuk mengenkripsi setiap kunci data. AWS Encryption SDK Mendukung tombol simetris AES dan tombol asimetris RSA dalam berbagai ukuran. Ini juga mendukung enkripsi AWS KMS keys simetris AWS Key Management Service(AWS KMS). Anda bertanggung jawab atas keamanan dan daya tahan kunci pembungkus Anda, jadi kami sarankan Anda menggunakan kunci enkripsi dalam modul keamanan perangkat keras atau layanan infrastruktur utama, seperti AWS KMS.

Untuk menentukan kunci pembungkus Anda untuk enkripsi dan dekripsi, Anda menggunakan keyring (C, Java,, .NET JavaScript, dan Python) atau penyedia kunci master (Java, Python, Encryption CLI). AWS Anda dapat menentukan satu kunci pembungkus atau beberapa kunci pembungkus dari jenis yang sama atau berbeda. Jika Anda menggunakan beberapa kunci pembungkus untuk membungkus kunci data, setiap kunci pembungkus akan mengenkripsi salinan kunci data yang sama. Kunci data terenkripsi (satu per kunci pembungkus) disimpan dengan data terenkripsi dalam pesan terenkripsi yang dikembalikan. AWS Encryption SDK Untuk mendekripsi data, pertama-tama AWS Encryption SDK harus menggunakan salah satu kunci pembungkus Anda untuk mendekripsi kunci data terenkripsi.

Untuk menentukan AWS KMS key dalam keyring atau penyedia kunci utama, gunakan pengenal AWS KMS kunci yang didukung. Untuk detail tentang pengidentifikasi kunci untuk AWS KMS kunci, lihat Pengidentifikasi Kunci di Panduan AWS Key Management Service Pengembang.

- Saat mengenkripsi dengan AWS Encryption SDK for Java,, AWS Encryption SDK for JavaScript, atau AWS CLI Enkripsi AWS Encryption SDK for Python, Anda dapat menggunakan pengidentifikasi kunci yang valid (ID kunci, ARN kunci, nama alias, atau alias ARN) untuk kunci KMS. Saat mengenkripsi dengan AWS Encryption SDK for C, Anda hanya dapat menggunakan ID kunci atau kunci ARN.

  Jika Anda menentukan nama alias atau alias ARN untuk kunci KMS saat mengenkripsi, menyimpan kunci ARN saat ini terkait dengan alias AWS Encryption SDK itu; itu tidak menyimpan alias. Perubahan pada alias tidak memengaruhi kunci KMS yang digunakan untuk mendekripsi kunci data Anda.

- Saat mendekripsi dalam mode ketat (di mana Anda menentukan kunci pembungkus tertentu), Anda harus menggunakan ARN kunci untuk mengidentifikasi. AWS KMS keys Persyaratan ini berlaku untuk semua implementasi bahasa dari. AWS Encryption SDK

  Ketika Anda mengenkripsi dengan AWS KMS keyring, AWS Encryption SDK menyimpan ARN kunci AWS KMS key dalam metadata kunci data terenkripsi. Saat mendekripsi dalam mode ketat, AWS Encryption SDK memverifikasi bahwa ARN kunci yang sama muncul di keyring (atau penyedia kunci utama) sebelum mencoba menggunakan kunci pembungkus untuk mendekripsi kunci data terenkripsi. Jika Anda menggunakan pengenal kunci yang berbeda, tidak AWS Encryption SDK akan mengenali atau menggunakan AWS KMS key, bahkan jika pengidentifikasi merujuk ke kunci yang sama.

Untuk menentukan kunci AES mentah atau key pair RSA mentah sebagai kunci pembungkus dalam keyring, Anda harus menentukan namespace dan nama. Dalam penyedia kunci master, `Provider ID` adalah setara dengan namespace dan setara dengan nama. `Key ID` Saat mendekripsi, Anda harus menggunakan namespace dan nama yang sama persis untuk setiap kunci pembungkus mentah seperti yang Anda gunakan saat mengenkripsi. Jika Anda menggunakan namespace atau nama yang berbeda, tidak AWS Encryption SDK akan mengenali atau menggunakan kunci pembungkus, meskipun materi kuncinya sama.

Menggunakan Multi-region AWS KMS keys

Anda dapat menggunakan AWS Key Management Service (AWS KMS) Tombol multi-region sebagai kunci pembungkus di. AWS Encryption SDK Jika Anda mengenkripsi dengan kunci Multi-wilayah dalam satu Wilayah AWS, Anda dapat mendekripsi menggunakan kunci Multi-wilayah terkait di yang berbeda. Wilayah AWS Support untuk kunci Multi-region diperkenalkan di versi 2.3. x dari AWS Encryption SDK dan versi 3.0. x dari CLI AWS Enkripsi.

AWS KMS Kunci multi-wilayah adalah satu set berbeda AWS KMS keys Wilayah AWS yang memiliki bahan kunci dan ID kunci yang sama. Anda dapat menggunakan kunci terkait ini seolah-olah mereka adalah kunci yang sama di Wilayah yang berbeda. Kunci Multi-Region mendukung pemulihan bencana umum dan skenario pencadangan yang memerlukan enkripsi di satu Wilayah dan mendekripsi di Wilayah yang berbeda tanpa melakukan panggilan Lintas wilayah. AWS KMS Untuk informasi tentang kunci Multi-region, lihat Menggunakan kunci Multi-region di Panduan AWS Key Management Service Pengembang.

Untuk mendukung kunci Multi-wilayah, AWS Encryption SDK termasuk gantungan kunci yang AWS KMS sadar Multi-wilayah dan penyedia kunci utama. multi-Region-awareSimbol baru dalam setiap bahasa pemrograman mendukung tombol Single-region dan Multi-region.

- Untuk kunci Single-region, multi-Region-aware simbol berperilaku seperti AWS KMS keyring wilayah tunggal dan penyedia kunci master. Ini mencoba untuk mendekripsi ciphertext hanya dengan kunci Single-region yang mengenkripsi data.
- Untuk kunci Multi-region, multi-Region-aware simbol mencoba mendekripsi ciphertext dengan kunci Multi-region yang sama yang mengenkripsi data atau dengan kunci replika Multi-wilayah terkait di Wilayah yang Anda tentukan.

Di multi-Region-aware keyrings dan penyedia kunci master yang mengambil lebih dari satu kunci KMS, Anda dapat menentukan beberapa kunci Single-region dan Multi-region. Namun, Anda hanya dapat menentukan satu kunci dari setiap set kunci replika Multi-wilayah terkait. Jika Anda menentukan lebih dari satu pengenal kunci dengan ID kunci yang sama, panggilan konstruktor gagal.

Anda juga dapat menggunakan kunci Multi-region dengan AWS KMS keyring standar, Single-region dan penyedia kunci master. Namun, Anda harus menggunakan kunci Multi-region yang sama di Wilayah yang sama untuk mengenkripsi dan mendekripsi. Keyring wilayah tunggal dan penyedia kunci utama mencoba mendekripsi ciphertext hanya dengan kunci yang mengenkripsi data.

Contoh berikut menunjukkan cara mengenkripsi dan mendekripsi data menggunakan kunci Multi-region dan multi-Region-aware keyrings baru dan penyedia kunci utama. Contoh-contoh ini mengenkripsi data di `us-east-1` Wilayah dan mendekripsi data di `us-west-2` Wilayah menggunakan kunci replika Multi-wilayah terkait di setiap Wilayah. Sebelum menjalankan contoh ini, ganti contoh Multi-region key ARN dengan nilai yang valid dari Anda. Akun AWS

C

Untuk mengenkripsi dengan kunci Multi-region, gunakan `Aws::Cryptosdk::KmsMrkAwareSymmetricKeyring::Builder()` metode ini untuk membuat instance keyring. Tentukan kunci Multi-wilayah.

Contoh sederhana ini tidak termasuk konteks enkripsi. Untuk contoh yang menggunakan konteks enkripsi di C, lihatMengenkripsi dan mendekripsi string.

Untuk contoh lengkap, lihat kms_multi_region_keys.cpp di AWS Encryption SDK for C repositori pada. GitHub

```
/* Encrypt with a multi-Region KMS key in us-east-1 */

/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();

/* Initialize a multi-Region keyring */
const char *mrk_us_east_1 = "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab";

struct aws_cryptosdk_keyring *mrk_keyring =
    Aws::Cryptosdk::KmsMrkAwareSymmetricKeyring::Builder().Build(mrk_us_east_1);

/* Create a session; release the keyring */
struct aws_cryptosdk_session *session =
    aws_cryptosdk_session_new_from_keyring_2(aws_default_allocator(),
 AWS_CRYPTOSDK_ENCRYPT, mrk_keyring);

aws_cryptosdk_keyring_release(mrk_keyring);

/* Encrypt the data
 *   aws_cryptosdk_session_process_full is designed for non-streaming data
 */
aws_cryptosdk_session_process_full(
    session, ciphertext, ciphertext_buf_sz, &ciphertext_len, plaintext,
 plaintext_len));

/* Clean up the session */
aws_cryptosdk_session_destroy(session);
```

C# / .NET

Untuk mengenkripsi dengan kunci Multi-region di Wilayah AS Timur (Virginia N.) (us-east-1), buat instance `CreateAwsKmsMrkKeyringInput` objek dengan pengenal kunci untuk kunci Multi-region dan klien untuk Wilayah yang ditentukan. AWS KMS Kemudian gunakan `CreateAwsKmsMrkKeyring()` metode untuk membuat keyring.

`CreateAwsKmsMrkKeyring()`Metode ini membuat keyring dengan tepat satu kunci Multi-region. Untuk mengenkripsi dengan beberapa kunci pembungkus, termasuk kunci Multi-wilayah, gunakan metode ini. `CreateAwsKmsMrkMultiKeyring()`

Untuk contoh lengkapnya, lihat AwsKmsMrkKeyringExample.cs di repositori.NET AWS Encryption SDK for. GitHub

```
//Encrypt with a multi-Region KMS key in us-east-1 Region

// Instantiate the AWS Encryption SDK and material providers
var encryptionSdk = AwsEncryptionSdkFactory.CreateDefaultAwsEncryptionSdk();
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders();


// Multi-Region keys have a distinctive key ID that begins with 'mrk'
// Specify a multi-Region key in us-east-1
string mrkUSEast1 = "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab";

// Create the keyring
// You can specify the Region or get the Region from the key ARN
var createMrkEncryptKeyringInput = new CreateAwsKmsMrkKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(RegionEndpoint.USEast1),
    KmsKeyId = mrkUSEast1
};
var mrkEncryptKeyring =
 materialProviders.CreateAwsKmsMrkKeyring(createMrkEncryptKeyringInput);

// Define the encryption context
var encryptionContext = new Dictionary<string, string>()
{
    {"purpose", "test"}
};

// Encrypt your plaintext data.
var encryptInput = new EncryptInput
{
    Plaintext = plaintext,
    Keyring = mrkEncryptKeyring,
    EncryptionContext = encryptionContext
};
var encryptOutput = encryptionSdk.Encrypt(encryptInput);
```

AWS Encryption CLI

Contoh ini mengenkripsi `hello.txt` file di bawah kunci Multi-region di Wilayah us-east-1. Karena contoh menentukan ARN kunci dengan elemen Region, contoh ini tidak menggunakan atribut region dari parameter. `--wrapping-keys`

Jika ID kunci dari kunci pembungkus tidak menentukan Wilayah, Anda dapat menggunakan atribut region `--wrapping-keys` untuk menentukan wilayah, seperti`--wrapping-keys key=$keyID region=us-east-1`.

```
# Encrypt with a multi-Region KMS key in us-east-1 Region

# To run this example, replace the fictitious key ARN with a valid value.
$ mrkUSEast1=arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --wrapping-keys key=$mrkUSEast1 \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --output .
```

Java

Untuk mengenkripsi dengan kunci Multi-region, buat instance `AwsKmsMrkAwareMasterKeyProvider` dan tentukan kunci Multi-region.

Untuk contoh lengkap, lihat BasicMultiRegionKeyEncryptionExample.javadi AWS Encryption SDK for Java repositori pada. GitHub

```
//Encrypt with a multi-Region KMS key in us-east-1 Region

// Instantiate the client
final AwsCrypto crypto = AwsCrypto.builder()
    .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
    .build();

// Multi-Region keys have a distinctive key ID that begins with 'mrk'
// Specify a multi-Region key in us-east-1
final String mrkUSEast1 = "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab";
```

```
// Instantiate an AWS KMS master key provider in strict mode for multi-Region keys
// Configure it to encrypt with the multi-Region key in us-east-1
final AwsKmsMrkAwareMasterKeyProvider kmsMrkProvider =
 AwsKmsMrkAwareMasterKeyProvider
    .builder()
    .buildStrict(mrkUSEast1);

// Create an encryption context
final Map<String, String> encryptionContext = Collections.singletonMap("Purpose",
 "Test");

// Encrypt your plaintext data
final CryptoResult<byte[], AwsKmsMrkAwareMasterKey> encryptResult =
 crypto.encryptData(
    kmsMrkProvider,
    encryptionContext,
    sourcePlaintext);
byte[] ciphertext = encryptResult.getResult();
```

JavaScript Browser

Untuk mengenkripsi dengan kunci Multi-region, gunakan `buildAwsKmsMrkAwareStrictMultiKeyringBrowser()` metode untuk membuat keyring dan tentukan kunci Multi-region.

Untuk contoh lengkap, lihat kms_multi_region_simple.ts di repositori pada. AWS Encryption SDK for JavaScript GitHub

```
/* Encrypt with a multi-Region KMS key in us-east-1 Region */

import {
  buildAwsKmsMrkAwareStrictMultiKeyringBrowser,
  buildClient,
  CommitmentPolicy,
  KMS,
} from '@aws-crypto/client-browser'


/* Instantiate an AWS Encryption SDK client */
const { encrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)
```

```
declare const credentials: {
  accessKeyId: string
  secretAccessKey: string
  sessionToken: string
}

/* Instantiate an AWS KMS client
 * The AWS Encryption SDK for JavaScript gets the Region from the key ARN
 */
const clientProvider = (region: string) => new KMS({ region, credentials })


/* Specify a multi-Region key in us-east-1 */
const multiRegionUsEastKey =
    'arn:aws:kms:us-east-1:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab'

/* Instantiate the keyring */
const encryptKeyring = buildAwsKmsMrkAwareStrictMultiKeyringBrowser({
    generatorKeyId: multiRegionUsEastKey,
    clientProvider,
  })


/* Set the encryption context */
const context = {
    purpose: 'test',
  }

/* Test data to encrypt */
const cleartext = new Uint8Array([1, 2, 3, 4, 5])

/* Encrypt the data */
const { result } = await encrypt(encryptKeyring, cleartext, {
    encryptionContext: context,
  })
```

JavaScript Node.js

Untuk mengenkripsi dengan kunci Multi-region, gunakan `buildAwsKmsMrkAwareStrictMultiKeyringNode()` metode untuk membuat keyring dan tentukan kunci Multi-region.

Untuk contoh lengkap, lihat kms_multi_region_simple.ts di repositori pada. AWS Encryption SDK for JavaScript GitHub

```
//Encrypt with a multi-Region KMS key in us-east-1 Region

import { buildClient } from '@aws-crypto/client-node'

/* Instantiate the AWS Encryption SDK client
const { encrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

/* Test string to encrypt */
const cleartext = 'asdf'

/* Multi-Region keys have a distinctive key ID that begins with 'mrk'
 * Specify a multi-Region key in us-east-1
 */
const multiRegionUsEastKey =
    'arn:aws:kms:us-east-1:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab'

/* Create an AWS KMS keyring */
const mrkEncryptKeyring = buildAwsKmsMrkAwareStrictMultiKeyringNode({
    generatorKeyId: multiRegionUsEastKey,
  })

/* Specify an encryption context */
const context = {
    purpose: 'test',
  }

/* Create an encryption keyring */
const { result } = await encrypt(mrkEncryptKeyring, cleartext, {
    encryptionContext: context,
  })
```

Python

Untuk mengenkripsi dengan kunci AWS KMS Multi-region, gunakan `MRKAwareStrictAwsKmsMasterKeyProvider()` metode dan tentukan kunci Multi-region.

Untuk contoh lengkap, lihat mrk_aware_kms_provider.py di AWS Encryption SDK for Python repositori pada. GitHub

```
* Encrypt with a multi-Region KMS key in us-east-1 Region

# Instantiate the client
client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_R

# Specify a multi-Region key in us-east-1
mrk_us_east_1 = "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"

# Use the multi-Region method to create the master key provider
# in strict mode
strict_mrk_key_provider = MRKAwareStrictAwsKmsMasterKeyProvider(
        key_ids=[mrk_us_east_1]
)

# Set the encryption context
encryption_context = {
        "purpose": "test"
    }

# Encrypt your plaintext data
ciphertext, encrypt_header = client.encrypt(
        source=source_plaintext,
        encryption_context=encryption_context,
        key_provider=strict_mrk_key_provider
)
```

Selanjutnya, pindahkan ciphertext Anda ke Region. `us-west-2` Anda tidak perlu mengenkripsi ulang ciphertext.

Untuk mendekripsi ciphertext dalam mode ketat di `us-west-2` Region, buat instance simbol multi-Region-aware dengan kunci ARN dari kunci Multi-region terkait di Region. `us-west-2` Jika Anda menentukan kunci ARN dari kunci Multi-wilayah terkait di Wilayah yang berbeda (termasuk`us-east-1`, di mana itu dienkripsi), multi-Region-aware simbol akan membuat panggilan lintas wilayah untuk itu. AWS KMS key

Saat mendekripsi dalam mode ketat, multi-Region-aware simbol membutuhkan kunci ARN. Ini hanya menerima satu ARN kunci dari setiap set kunci Multi-wilayah terkait.

Sebelum menjalankan contoh ini, ganti contoh Multi-region key ARN dengan nilai yang valid dari Anda. Akun AWS

C

Untuk mendekripsi dalam mode ketat dengan kunci Multi-region, gunakan `Aws::Cryptosdk::KmsMrkAwareSymmetricKeyring::Builder()` metode ini untuk membuat instance keyring. Tentukan kunci Multi-wilayah terkait di Wilayah lokal (us-west-2).

Untuk contoh lengkap, lihat kms_multi_region_keys.cpp di AWS Encryption SDK for C repositori pada. GitHub

```
/* Decrypt with a related multi-Region KMS key in us-west-2 Region */

/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();

/* Initialize a multi-Region keyring */
const char *mrk_us_west_2 = "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab";

struct aws_cryptosdk_keyring *mrk_keyring =
    Aws::Cryptosdk::KmsMrkAwareSymmetricKeyring::Builder().Build(mrk_us_west_2);

/* Create a session; release the keyring */
struct aws_cryptosdk_session *session =
    aws_cryptosdk_session_new_from_keyring_2(aws_default_allocator(),
 AWS_CRYPTOSDK_ENCRYPT, mrk_keyring);

aws_cryptosdk_session_set_commitment_policy(session,
    COMMITMENT_POLICY_REQUIRE_ENCRYPT_REQUIRE_DECRYPT);

aws_cryptosdk_keyring_release(mrk_keyring);

/* Decrypt the ciphertext
 *   aws_cryptosdk_session_process_full is designed for non-streaming data
 */
aws_cryptosdk_session_process_full(
    session, plaintext, plaintext_buf_sz, &plaintext_len, ciphertext,
 ciphertext_len));

/* Clean up the session */
aws_cryptosdk_session_destroy(session);
```

C# / .NET

Untuk mendekripsi dalam mode ketat dengan satu kunci Multi-wilayah, gunakan konstruktor dan metode yang sama yang Anda gunakan untuk merakit input dan membuat keyring untuk mengenkripsi. Buat instance `CreateAwsKmsMrkKeyringInput` objek dengan ARN kunci dari kunci Multi-wilayah terkait dan AWS KMS klien untuk Wilayah AS Barat (Oregon) (us-west-2). Kemudian gunakan `CreateAwsKmsMrkKeyring()` metode untuk membuat keyring Multi-wilayah dengan satu kunci KMS Multi-wilayah.

Untuk contoh lengkapnya, lihat AwsKmsMrkKeyringExample.cs di repositori.NET AWS Encryption SDK for. GitHub

```
// Decrypt with a related multi-Region KMS key in us-west-2 Region

// Instantiate the AWS Encryption SDK and material providers
var encryptionSdk = AwsEncryptionSdkFactory.CreateDefaultAwsEncryptionSdk();
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders();

// Specify the key ARN of the multi-Region key in us-west-2
string mrkUSWest2 = "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab";

// Instantiate the keyring input
// You can specify the Region or get the Region from the key ARN
var createMrkDecryptKeyringInput = new CreateAwsKmsMrkKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(RegionEndpoint.USWest2),
    KmsKeyId = mrkUSWest2
};

// Create the multi-Region keyring
var mrkDecryptKeyring =
 materialProviders.CreateAwsKmsMrkKeyring(createMrkDecryptKeyringInput);

// Decrypt the ciphertext
var decryptInput = new DecryptInput
{
    Ciphertext = ciphertext,
    Keyring = mrkDecryptKeyring
};
```

```
var decryptOutput = encryptionSdk.Decrypt(decryptInput);
```

AWS Encryption CLI

Untuk mendekripsi dengan kunci Multi-region terkait di Wilayah us-west-2, gunakan atribut kunci parameter untuk menentukan ARN kuncinya. `--wrapping-keys`

```
# Decrypt with a related multi-Region KMS key in us-west-2 Region

# To run this example, replace the fictitious key ARN with a valid value.
$ mrkUSWest2=arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys key=$mrkUSWest2 \
                     --commitment-policy require-encrypt-require-decrypt \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --max-encrypted-data-keys 1 \
                     --buffer \
                     --output .
```

Java

Untuk mendekripsi dalam mode ketat, buat instance `AwsKmsMrkAwareMasterKeyProvider` dan tentukan kunci Multi-wilayah terkait di Wilayah lokal (us-west-2).

Untuk contoh lengkap, lihat BasicMultiRegionKeyEncryptionExample.java di AWS Encryption SDK for Java repositori pada. GitHub

```
// Decrypt with a related multi-Region KMS key in us-west-2 Region

// Instantiate the client
final AwsCrypto crypto = AwsCrypto.builder()
    .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
    .build();

// Related multi-Region keys have the same key ID. Their key ARNs differs only in
 the Region field.
String mrkUSWest2 = "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab";
```

```
// Use the multi-Region method to create the master key provider
// in strict mode
AwsKmsMrkAwareMasterKeyProvider kmsMrkProvider =
 AwsKmsMrkAwareMasterKeyProvider.builder()
    .buildStrict(mrkUSWest2);

// Decrypt your ciphertext
CryptoResult<byte[], AwsKmsMrkAwareMasterKey> decryptResult = crypto.decryptData(
        kmsMrkProvider,
        ciphertext);
byte[] decrypted = decryptResult.getResult();
```

JavaScript Browser

Untuk mendekripsi dalam mode ketat, gunakan `buildAwsKmsMrkAwareStrictMultiKeyringBrowser()` metode untuk membuat keyring dan tentukan kunci Multi-region terkait di Wilayah lokal (us-west-2).

Untuk contoh lengkap, lihat kms_multi_region_simple.ts di repositori pada. AWS Encryption SDK for JavaScript GitHub

```
/* Decrypt with a related multi-Region KMS key in us-west-2 Region */

import {
  buildAwsKmsMrkAwareStrictMultiKeyringBrowser,
  buildClient,
  CommitmentPolicy,
  KMS,
} from '@aws-crypto/client-browser'


/* Instantiate an AWS Encryption SDK client */
const { decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

declare const credentials: {
  accessKeyId: string
  secretAccessKey: string
  sessionToken: string
}

/* Instantiate an AWS KMS client
```

```
 * The AWS Encryption SDK for JavaScript gets the Region from the key ARN
 */
const clientProvider = (region: string) => new KMS({ region, credentials })


/* Specify a multi-Region key in us-west-2 */
const multiRegionUsWestKey =
    'arn:aws:kms:us-west-2:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab'

/* Instantiate the keyring */
const mrkDecryptKeyring = buildAwsKmsMrkAwareStrictMultiKeyringBrowser({
    generatorKeyId: multiRegionUsWestKey,
    clientProvider,
  })


/* Decrypt the data */
const { plaintext, messageHeader } = await decrypt(mrkDecryptKeyring, result)
```

JavaScript Node.js

Untuk mendekripsi dalam mode ketat, gunakan `buildAwsKmsMrkAwareStrictMultiKeyringNode()` metode untuk membuat keyring dan tentukan kunci Multi-region terkait di Wilayah lokal (us-west-2).

Untuk contoh lengkap, lihat kms_multi_region_simple.ts di repositori pada. AWS Encryption SDK for JavaScript GitHub

```
/* Decrypt with a related multi-Region KMS key in us-west-2 Region */

import { buildClient } from '@aws-crypto/client-node'

/* Instantiate the client
const { decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

/* Multi-Region keys have a distinctive key ID that begins with 'mrk'
 * Specify a multi-Region key in us-west-2
 */
const multiRegionUsWestKey =
    'arn:aws:kms:us-west-2:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab'
```

```
/* Create an AWS KMS keyring */
const mrkDecryptKeyring = buildAwsKmsMrkAwareStrictMultiKeyringNode({
    generatorKeyId: multiRegionUsWestKey,
  })

/* Decrypt your ciphertext */
const { plaintext, messageHeader } = await decrypt(decryptKeyring, result)
```

Python

Untuk mendekripsi dalam mode ketat, gunakan `MRKAwareStrictAwsKmsMasterKeyProvider()` metode untuk membuat penyedia kunci master. Tentukan kunci Multi-wilayah terkait di Wilayah lokal (us-west-2).

Untuk contoh lengkap, lihat mrk_aware_kms_provider.py di AWS Encryption SDK for Python repositori pada. GitHub

```
# Decrypt with a related multi-Region KMS key in us-west-2 Region

# Instantiate the client
client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_R

# Related multi-Region keys have the same key ID. Their key ARNs differs only in the
 Region field
mrk_us_west_2 = "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"

# Use the multi-Region method to create the master key provider
# in strict mode
strict_mrk_key_provider = MRKAwareStrictAwsKmsMasterKeyProvider(
        key_ids=[mrk_us_west_2]
)

# Decrypt your ciphertext
plaintext, _ = client.decrypt(
        source=ciphertext,
        key_provider=strict_mrk_key_provider
)
```

Anda juga dapat mendekripsi dalam mode penemuan dengan tombol AWS KMS Multi-wilayah. Saat mendekripsi dalam mode penemuan, Anda tidak menentukan apa pun. AWS KMS keys(Untuk

informasi tentang gantungan kunci AWS KMS penemuan wilayah tunggal, lihatMenggunakan AWS KMS keyring penemuan.)

Jika Anda dienkripsi dengan kunci Multi-region, multi-Region-aware simbol dalam mode penemuan akan mencoba mendekripsi dengan menggunakan kunci Multi-wilayah terkait di Wilayah lokal. Jika tidak ada; panggilan gagal. Dalam mode penemuan, tidak AWS Encryption SDK akan mencoba panggilan lintas wilayah untuk kunci Multi-wilayah yang digunakan untuk enkripsi.

> **Note**
>
> Jika Anda menggunakan multi-Region-aware simbol dalam mode penemuan untuk mengenkripsi data, operasi enkripsi gagal.

Contoh berikut menunjukkan cara mendekripsi dengan multi-Region-aware simbol dalam mode penemuan. Karena Anda tidak menentukan AWS KMS key, AWS Encryption SDK harus mendapatkan Wilayah dari sumber yang berbeda. Jika memungkinkan, tentukan Wilayah lokal secara eksplisit. Jika tidak, AWS Encryption SDK akan mendapatkan Wilayah lokal dari Wilayah yang dikonfigurasi dalam AWS SDK untuk bahasa pemrograman Anda.

Sebelum menjalankan contoh ini, ganti contoh ID akun dan ARN kunci Multi-wilayah dengan nilai yang valid dari Anda. Akun AWS

C

Untuk mendekripsi dalam mode penemuan dengan kunci Multi-region, gunakan `Aws::Cryptosdk::KmsMrkAwareSymmetricKeyring::Builder()` metode untuk membangun keyring, dan `Aws::Cryptosdk::KmsKeyring::DiscoveryFilter::Builder()` metode untuk membangun filter penemuan. Untuk menentukan Wilayah lokal, tentukan `ClientConfiguration` dan tentukan di AWS KMS klien.

Untuk contoh lengkap, lihat kms_multi_region_keys.cpp di AWS Encryption SDK for C repositori pada. GitHub

```
/* Decrypt in discovery mode with a multi-Region KMS key */

/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();
```

```
/* Construct a discovery filter for the account and partition. The
 *  filter is optional, but it's a best practice that we recommend.
 */
const char *account_id = "111122223333";
const char *partition = "aws";
const std::shared_ptr<Aws::Cryptosdk::KmsKeyring::DiscoveryFilter> discovery_filter
 =

 Aws::Cryptosdk::KmsKeyring::DiscoveryFilter::Builder(partition).AddAccount(account_id).Buil

/* Create an AWS KMS client in the desired region. */
const char *region = "us-west-2";

Aws::Client::ClientConfiguration client_config;
client_config.region = region;
const std::shared_ptr<Aws::KMS::KMSClient> kms_client =
    Aws::MakeShared<Aws::KMS::KMSClient>("AWS_SAMPLE_CODE", client_config);

struct aws_cryptosdk_keyring *mrk_keyring =
    Aws::Cryptosdk::KmsMrkAwareSymmetricKeyring::Builder()
        .WithKmsClient(kms_client)
        .BuildDiscovery(region, discovery_filter);

/* Create a session; release the keyring */
struct aws_cryptosdk_session *session =
    aws_cryptosdk_session_new_from_keyring_2(aws_default_allocator(),
 AWS_CRYPTOSDK_DECRYPT, mrk_keyring);

aws_cryptosdk_keyring_release(mrk_keyring);
commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
/* Decrypt the ciphertext
 *   aws_cryptosdk_session_process_full is designed for non-streaming data
 */
aws_cryptosdk_session_process_full(
    session, plaintext, plaintext_buf_sz, &plaintext_len, ciphertext,
 ciphertext_len));

/* Clean up the session */
aws_cryptosdk_session_destroy(session);
```

C# / .NET

Untuk membuat keyring multi-Region-aware penemuan di AWS Encryption SDK for .NET, buat instance `CreateAwsKmsMrkDiscoveryKeyringInput` objek yang mengambil AWS KMS klien

untuk tertentu Wilayah AWS, dan filter penemuan opsional yang membatasi kunci KMS ke partisi dan akun tertentu AWS . Kemudian panggil `CreateAwsKmsMrkDiscoveryKeyring()` metode dengan objek input. Untuk contoh lengkapnya, lihat AwsKmsMrkDiscoveryKeyringExample.cs di repositori.NET AWS Encryption SDK for. GitHub

Untuk membuat keyring multi-Region-aware penemuan untuk lebih dari satu Wilayah AWS, gunakan `CreateAwsKmsMrkDiscoveryMultiKeyring()` metode ini untuk membuat multi-keyring, atau gunakan `CreateAwsKmsMrkDiscoveryKeyring()` untuk membuat beberapa keyring multi-Region-aware penemuan dan kemudian gunakan `CreateMultiKeyring()` metode untuk menggabungkannya dalam multi-keyring.

Sebagai contoh, lihat AwsKmsMrkDiscoveryMultiKeyringExample.cs.

```
// Decrypt in discovery mode with a multi-Region KMS key

// Instantiate the AWS Encryption SDK and material providers
var encryptionSdk = AwsEncryptionSdkFactory.CreateDefaultAwsEncryptionSdk();
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders();

List<string> account = new List<string> { "111122223333" };

// Instantiate the discovery filter
DiscoveryFilter mrkDiscoveryFilter = new DiscoveryFilter()
{
    AccountIds = account,
    Partition = "aws"
}

// Create the keyring
var createMrkDiscoveryKeyringInput = new CreateAwsKmsMrkDiscoveryKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(RegionEndpoint.USWest2),
    DiscoveryFilter = mrkDiscoveryFilter
};
var mrkDiscoveryKeyring =
 materialProviders.CreateAwsKmsMrkDiscoveryKeyring(createMrkDiscoveryKeyringInput);


// Decrypt the ciphertext
var decryptInput = new DecryptInput
```

```
{
    Ciphertext = ciphertext,
    Keyring = mrkDiscoveryKeyring
};
var decryptOutput = encryptionSdk.Decrypt(decryptInput);
```

AWS Encryption CLI

Untuk mendekripsi dalam mode penemuan, gunakan atribut penemuan parameter. `--wrapping-keys` Atribut discovery-account dan discovery-partition membuat filter penemuan yang opsional, tetapi direkomendasikan.

Untuk menentukan Region, perintah ini mencakup atribut region dari `--wrapping-keys` parameter.

```
# Decrypt in discovery mode with a multi-Region KMS key

$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys discovery=true \
                                     discovery-account=111122223333 \
                                     discovery-partition=aws \
                                     region=us-west-2 \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --max-encrypted-data-keys 1 \
                     --buffer \
                     --output .
```

Java

Untuk menentukan Wilayah lokal, gunakan `builder().withDiscoveryMrkRegion` parameter. Jika tidak, AWS Encryption SDK mendapatkan Wilayah lokal dari Wilayah yang dikonfigurasi di AWS SDK for Java.

Untuk contoh lengkap, lihat DiscoveryMultiRegionDecryptionExample.java di AWS Encryption SDK for Java repositori pada. GitHub

```
// Decrypt in discovery mode with a multi-Region KMS key

// Instantiate the client
final AwsCrypto crypto = AwsCrypto.builder()
    .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
```

```
    .build();

DiscoveryFilter discoveryFilter = new DiscoveryFilter("aws", 111122223333);

AwsKmsMrkAwareMasterKeyProvider mrkDiscoveryProvider =
 AwsKmsMrkAwareMasterKeyProvider
    .builder()
    .withDiscoveryMrkRegion(Region.US_WEST_2)
    .buildDiscovery(discoveryFilter);

// Decrypt your ciphertext
final CryptoResult<byte[], AwsKmsMrkAwareMasterKey> decryptResult = crypto
    .decryptData(mrkDiscoveryProvider, ciphertext);
```

JavaScript Browser

Untuk mendekripsi dalam mode penemuan dengan kunci Multi-region simetris, gunakan metode ini. `AwsKmsMrkAwareSymmetricDiscoveryKeyringBrowser()`

Untuk contoh lengkap, lihat kms_multi_region_discovery.ts di repositori pada. AWS Encryption SDK for JavaScript GitHub

```
/* Decrypt in discovery mode with a multi-Region KMS key */

import {
  AwsKmsMrkAwareSymmetricDiscoveryKeyringBrowser,
  buildClient,
  CommitmentPolicy,
  KMS,
} from '@aws-crypto/client-browser'


/* Instantiate an AWS Encryption SDK client */
const { decrypt } = buildClient()

declare const credentials: {
  accessKeyId: string
  secretAccessKey: string
  sessionToken: string
}

/* Instantiate the KMS client with an explicit Region */
const client = new KMS({ region: 'us-west-2', credentials })
```

```
/* Create a discovery filter */
const discoveryFilter = { partition: 'aws', accountIDs: ['111122223333'] }


/* Create an AWS KMS discovery keyring */
const mrkDiscoveryKeyring = new AwsKmsMrkAwareSymmetricDiscoveryKeyringBrowser({
    client,
    discoveryFilter,
  })


/* Decrypt the data */
const { plaintext, messageHeader } = await decrypt(mrkDiscoveryKeyring, ciphertext)
```

JavaScript Node.js

Untuk mendekripsi dalam mode penemuan dengan kunci Multi-region simetris, gunakan metode ini. `AwsKmsMrkAwareSymmetricDiscoveryKeyringNode()`

Untuk contoh lengkap, lihat kms_multi_region_discovery.ts di repositori pada. AWS Encryption SDK for JavaScript GitHub

```
/* Decrypt in discovery mode with a multi-Region KMS key */

import {
  AwsKmsMrkAwareSymmetricDiscoveryKeyringNode,
  buildClient,
  CommitmentPolicy,
  KMS,
} from '@aws-crypto/client-node'

/* Instantiate the Encryption SDK client
const { decrypt } = buildClient()

/* Instantiate the KMS client with an explicit Region */
const client = new KMS({ region: 'us-west-2' })

/* Create a discovery filter */
const discoveryFilter = { partition: 'aws', accountIDs: ['111122223333'] }

/* Create an AWS KMS discovery keyring */
```

```
const mrkDiscoveryKeyring = new AwsKmsMrkAwareSymmetricDiscoveryKeyringNode({
    client,
    discoveryFilter,
  })

/* Decrypt your ciphertext */
const { plaintext, messageHeader } = await decrypt(mrkDiscoveryKeyring, result)
```

Python

Untuk mendekripsi dalam mode penemuan dengan kunci Multi-wilayah, gunakan metode ini. `MRKAwareDiscoveryAwsKmsMasterKeyProvider()`

Untuk contoh lengkap, lihat mrk_aware_kms_provider.py di AWS Encryption SDK for Python repositori pada. GitHub

```
# Decrypt in discovery mode with a multi-Region KMS key

# Instantiate the client
client = aws_encryption_sdk.EncryptionSDKClient()

# Create the discovery filter and specify the region
decrypt_kwargs = dict(
        discovery_filter=DiscoveryFilter(account_ids="111122223333",
 partition="aws"),
        discovery_region="us-west-2",
    )

# Use the multi-Region method to create the master key provider
# in discovery mode
mrk_discovery_key_provider =
 MRKAwareDiscoveryAwsKmsMasterKeyProvider(**decrypt_kwargs)

# Decrypt your ciphertext
plaintext, _ = client.decrypt(
        source=ciphertext,
        key_provider=mrk_discovery_key_provider
)
```

Memilih rangkaian algoritme

AWS Encryption SDK Mendukung beberapa algoritma enkripsi simetris dan asimetris untuk mengenkripsi kunci data Anda di bawah kunci pembungkus yang Anda tentukan. Namun, ketika menggunakan kunci data tersebut untuk mengenkripsi data Anda, AWS Encryption SDK default ke rangkaian algoritme yang direkomendasikan yang menggunakan algoritma AES-GCM dengan derivasi kunci, tanda tangan digital, dan komitmen kunci. Meskipun rangkaian algoritme default kemungkinan cocok untuk sebagian besar aplikasi, Anda dapat memilih rangkaian algoritme alternatif. Misalnya, beberapa model kepercayaan akan dipenuhi oleh rangkaian algoritma tanpa tanda tangan digital. Untuk informasi tentang rangkaian algoritme yang AWS Encryption SDK didukung, lihatSuite algoritma yang didukung di AWS Encryption SDK.

Contoh berikut menunjukkan cara memilih rangkaian algoritma alternatif saat mengenkripsi. Contoh-contoh ini memilih rangkaian algoritma AES-GCM yang direkomendasikan dengan derivasi kunci dan komitmen kunci, tetapi tanpa tanda tangan digital. Saat Anda mengenkripsi dengan rangkaian algoritme yang tidak menyertakan tanda tangan digital, gunakan mode dekripsi khusus tanpa tanda tangan saat mendekripsi. Mode ini, yang gagal jika menemukan ciphertext yang ditandatangani, paling berguna saat streaming dekripsi.

C

Untuk menentukan rangkaian algoritma alternatif di AWS Encryption SDK for C, Anda harus membuat CMM secara eksplisit. Kemudian gunakan `aws_cryptosdk_default_cmm_set_alg_id` with the CMM dan suite algoritma yang dipilih.

```
/* Specify an algorithm suite without signing */

/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();

/* Construct an AWS KMS keyring */
struct aws_cryptosdk_keyring *kms_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn);

/* To set an alternate algorithm suite, create an cryptographic
   materials manager (CMM) explicitly
 */
struct aws_cryptosdk_cmm *cmm =
 aws_cryptosdk_default_cmm_new(aws_default_allocator(), kms_keyring);
aws_cryptosdk_keyring_release(kms_keyring);
```

```
/* Specify the algorithm suite for the CMM */
aws_cryptosdk_default_cmm_set_alg_id(cmm, ALG_AES256_GCM_HKDF_SHA512_COMMIT_KEY);

/* Construct the session with the CMM,
   then release the CMM reference
 */
struct aws_cryptosdk_session *session = aws_cryptosdk_session_new_from_cmm_2(alloc,
 AWS_CRYPTOSDK_ENCRYPT, cmm);
aws_cryptosdk_cmm_release(cmm);

/* Encrypt the data
   Use aws_cryptosdk_session_process_full with non-streaming data
 */
if (AWS_OP_SUCCESS != aws_cryptosdk_session_process_full(
                          session,
                          ciphertext,
                          ciphertext_buf_sz,
                          &ciphertext_len,
                          plaintext,
                          plaintext_len)) {
    aws_cryptosdk_session_destroy(session);
    return AWS_OP_ERR;
}
```

Saat mendekripsi data yang dienkripsi tanpa tanda tangan digital, gunakan. `AWS_CRYPTOSDK_DECRYPT_UNSIGNED` Hal ini menyebabkan dekripsi gagal jika menemukan ciphertext yang ditandatangani.

```
/* Decrypt unsigned streaming data */

/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();

/* Construct an AWS KMS keyring */
struct aws_cryptosdk_keyring *kms_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn);

/* Create a session for decrypting with the AWS KMS keyring
   Then release the keyring reference
 */
struct aws_cryptosdk_session *session =
```

```
 aws_cryptosdk_session_new_from_keyring_2(alloc, AWS_CRYPTOSDK_DECRYPT_UNSIGNED,
 kms_keyring);
aws_cryptosdk_keyring_release(kms_keyring);

if (!session) {
    return AWS_OP_ERR;
}

/* Limit encrypted data keys */
aws_cryptosdk_session_set_max_encrypted_data_keys(session, 1);

/* Decrypt
   Use aws_cryptosdk_session_process_full with non-streaming data
 */
    if (AWS_OP_SUCCESS != aws_cryptosdk_session_process_full(
                          session,
                          plaintext,
                          plaintext_buf_sz,
                          &plaintext_len,
                          ciphertext,
                          ciphertext_len)) {
    aws_cryptosdk_session_destroy(session);
    return AWS_OP_ERR;
}
```

C# / .NET

Untuk menentukan rangkaian algoritme alternatif di AWS Encryption SDK for .NET, tentukan `AlgorithmSuiteId` properti EncryptInputobjek. AWS Encryption SDK Untuk .NET mencakup konstanta yang dapat Anda gunakan untuk mengidentifikasi rangkaian algoritme pilihan Anda.

The AWS Encryption SDK for .NET tidak memiliki metode untuk mendeteksi ciphertext yang ditandatangani saat streaming dekripsi karena pustaka ini tidak mendukung data streaming.

```
// Specify an algorithm suite without signing

// Instantiate the AWS Encryption SDK and material providers
var encryptionSdk = AwsEncryptionSdkFactory.CreateDefaultAwsEncryptionSdk();
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders();
```

```
// Create the keyring
var keyringInput = new CreateAwsKmsKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = keyArn
};
var keyring = materialProviders.CreateAwsKmsKeyring(keyringInput);

// Encrypt your plaintext data
var encryptInput = new EncryptInput
{
    Plaintext = plaintext,
    Keyring = keyring,
    AlgorithmSuiteId = AlgorithmSuiteId.ALG_AES_256_GCM_HKDF_SHA512_COMMIT_KEY
};
var encryptOutput = encryptionSdk.Encrypt(encryptInput);
```

AWS Encryption CLI

Saat mengenkripsi `hello.txt` file, contoh ini menggunakan `--algorithm` parameter untuk menentukan rangkaian algoritma tanpa tanda tangan digital.

```
# Specify an algorithm suite without signing

# To run this example, replace the fictitious key ARN with a valid value.
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --wrapping-keys key=$keyArn \
                     --algorithm AES_256_GCM_HKDF_SHA512_COMMIT_KEY \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --commitment-policy require-encrypt-require-decrypt \
                     --output hello.txt.encrypted \
                     --decode
```

Saat mendekripsi, contoh ini menggunakan parameter. `--decrypt-unsigned` Parameter ini disarankan untuk memastikan bahwa Anda mendekripsi ciphertext yang tidak ditandatangani, terutama dengan CLI, yang selalu streaming input dan output.

```
# Decrypt unsigned streaming data
```

```
# To run this example, replace the fictitious key ARN with a valid value.
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$ aws-encryption-cli --decrypt-unsigned \
                     --input hello.txt.encrypted \
                     --wrapping-keys key=$keyArn \
                     --max-encrypted-data-keys 1 \
                     --commitment-policy require-encrypt-require-decrypt \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --output .
```

Java

Untuk menentukan rangkaian algoritma alternatif, gunakan `AwsCrypto.builder().withEncryptionAlgorithm()` metode ini. Contoh ini menentukan rangkaian algoritma alternatif tanpa tanda tangan digital.

```
// Specify an algorithm suite without signing

// Instantiate the client
AwsCrypto crypto = AwsCrypto.builder()
    .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
    .withEncryptionAlgorithm(CryptoAlgorithm.ALG_AES_256_GCM_HKDF_SHA512_COMMIT_KEY)
    .build();

String awsKmsKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Create a master key provider in strict mode
KmsMasterKeyProvider masterKeyProvider = KmsMasterKeyProvider.builder()
    .buildStrict(awsKmsKey);

// Create an encryption context to identify this ciphertext
        Map<String, String> encryptionContext = Collections.singletonMap("Example",
 "FileStreaming");

// Encrypt your plaintext data
CryptoResult<byte[], KmsMasterKey> encryptResult = crypto.encryptData(
    masterKeyProvider,
    sourcePlaintext,
    encryptionContext);
```

```
byte[] ciphertext = encryptResult.getResult();
```

Saat streaming data untuk dekripsi, gunakan `createUnsignedMessageDecryptingStream()` metode ini untuk memastikan bahwa semua ciphertext yang Anda dekripsi tidak ditandatangani.

```
// Decrypt unsigned streaming data

// Instantiate the client
AwsCrypto crypto = AwsCrypto.builder()
  .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
  .withMaxEncryptedDataKeys(1)
  .build();

// Create a master key provider in strict mode
String awsKmsKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
KmsMasterKeyProvider masterKeyProvider = KmsMasterKeyProvider.builder()
  .buildStrict(awsKmsKey);

// Decrypt the encrypted message
FileInputStream in = new FileInputStream(srcFile + ".encrypted");
CryptoInputStream<KmsMasterKey> decryptingStream =
 crypto.createUnsignedMessageDecryptingStream(masterKeyProvider, in);

// Return the plaintext data
// Write the plaintext data to disk
FileOutputStream out = new FileOutputStream(srcFile + ".decrypted");
IOUtils.copy(decryptingStream, out);
decryptingStream.close();
```

JavaScript Browser

Untuk menentukan rangkaian algoritma alternatif, gunakan `suiteId` parameter dengan nilai `AlgorithmSuiteIdentifier` enum.

```
// Specify an algorithm suite without signing

// Instantiate the client
const { encrypt } = buildClient( CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT )

// Specify a KMS key
const generatorKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
// Create a keyring with the KMS key
const keyring = new KmsKeyringBrowser({ generatorKeyId })

// Encrypt your plaintext data
const { result } = await encrypt(keyring, cleartext, { suiteId:
 AlgorithmSuiteIdentifier.ALG_AES256_GCM_IV12_TAG16_HKDF_SHA512_COMMIT_KEY,
 encryptionContext: context, })
```

Saat mendekripsi, gunakan metode standar`decrypt`. AWS Encryption SDK for JavaScript di browser tidak memiliki `decrypt-unsigned` mode karena browser tidak mendukung streaming.

```
// Decrypt unsigned streaming data

// Instantiate the client
const { decrypt } = buildClient( CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT )

// Create a keyring with the same KMS key used to encrypt
const generatorKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
const keyring = new KmsKeyringBrowser({ generatorKeyId })

// Decrypt the encrypted message
const { plaintext, messageHeader } = await decrypt(keyring, ciphertextMessage)
```

JavaScript Node.js

Untuk menentukan rangkaian algoritma alternatif, gunakan `suiteId` parameter dengan nilai `AlgorithmSuiteIdentifier` enum.

```
// Specify an algorithm suite without signing

// Instantiate the client
const { encrypt } = buildClient( CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT )

// Specify a KMS key
const generatorKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Create a keyring with the KMS key
const keyring = new KmsKeyringNode({ generatorKeyId })

// Encrypt your plaintext data
```

```
const { result } = await encrypt(keyring, cleartext, { suiteId:
 AlgorithmSuiteIdentifier.ALG_AES256_GCM_IV12_TAG16_HKDF_SHA512_COMMIT_KEY,
 encryptionContext: context, })
```

Saat mendekripsi data yang dienkripsi tanpa tanda tangan digital, gunakan Stream. decryptUnsignedMessage Metode ini gagal jika menemukan ciphertext yang ditandatangani.

```
// Decrypt unsigned streaming data

// Instantiate the client
const { decryptUnsignedMessageStream } =
 buildClient( CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT )

// Create a keyring with the same KMS key used to encrypt
const generatorKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
const keyring = new KmsKeyringNode({ generatorKeyId })

// Decrypt the encrypted message
const outputStream =
 createReadStream(filename) .pipe(decryptUnsignedMessageStream(keyring))
```

Python

Untuk menentukan algoritma enkripsi alternatif, gunakan `algorithm` parameter dengan nilai `Algorithm` enum.

```
# Specify an algorithm suite without signing

# Instantiate a client
client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_R
                                                max_encrypted_data_keys=1)

# Create a master key provider in strict mode
aws_kms_key = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
aws_kms_strict_master_key_provider = StrictAwsKmsMasterKeyProvider(
        key_ids=[aws_kms_key]
)

# Encrypt the plaintext using an alternate algorithm suite
ciphertext, encrypted_message_header = client.encrypt(
```

```
    algorithm=Algorithm.AES_256_GCM_HKDF_SHA512_COMMIT_KEY, source=source_plaintext,
 key_provider=kms_key_provider
)
```

Saat mendekripsi pesan yang dienkripsi tanpa tanda tangan digital, gunakan mode `decrypt-unsigned` streaming, terutama saat mendekripsi saat streaming.

```
# Decrypt unsigned streaming data

# Instantiate the client
client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_R
                                                    max_encrypted_data_keys=1)

# Create a master key provider in strict mode
aws_kms_key = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
aws_kms_strict_master_key_provider = StrictAwsKmsMasterKeyProvider(
        key_ids=[aws_kms_key]
)

# Decrypt with decrypt-unsigned
with open(ciphertext_filename, "rb") as ciphertext, open(cycled_plaintext_filename,
 "wb") as plaintext:
    with client.stream(mode="decrypt-unsigned",
                       source=ciphertext,
                       key_provider=master_key_provider) as decryptor:
        for chunk in decryptor:
            plaintext.write(chunk)

# Verify that the encryption context
assert all(
   pair in decryptor.header.encryption_context.items() for pair in
 encryptor.header.encryption_context.items()
)
return ciphertext_filename, cycled_plaintext_filename
```

Rust

Untuk menentukan rangkaian algoritme alternatif di AWS Encryption SDK for Rust, tentukan `algorithm_suite_id` properti dalam permintaan enkripsi Anda.

```
// Instantiate the AWS Encryption SDK client
```

```
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Define the key namespace and key name
let key_namespace: &str = "HSM_01";
let key_name: &str = "AES_256_012";

// Optional: Create an encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create Raw AES keyring
let raw_aes_keyring = mpl
    .create_raw_aes_keyring()
    .key_name(key_name)
    .key_namespace(key_namespace)
    .wrapping_key(aws_smithy_types::Blob::new(AESWrappingKey))
    .wrapping_alg(AesWrappingAlg::AlgAes256GcmIv12Tag16)
    .send()
    .await?;

// Encrypt your plaintext data
let plaintext = example_data.as_bytes();

let encryption_response = esdk_client.encrypt()
    .plaintext(plaintext)
    .keyring(raw_aes_keyring.clone())
    .encryption_context(encryption_context.clone())
    .algorithm_suite_id(AlgAes256GcmHkdfSha512CommitKey)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)
// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Define the key namespace and key name
var keyNamespace = "HSM_01"
var keyName = "AES_256_012"

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create Raw AES keyring
aesKeyRingInput := mpltypes.CreateRawAesKeyringInput{
    KeyName:      keyName,
    KeyNamespace: keyNamespace,
    WrappingKey:  key,
```

```
    WrappingAlg:  mpltypes.AesWrappingAlgAlgAes256GcmIv12Tag16,
}
aesKeyring, err := matProv.CreateRawAesKeyring(context.Background(),
 aesKeyRingInput)
if err != nil {
    panic(err)
}

// Encrypt your plaintext data
algorithmSuiteId := mpltypes.ESDKAlgorithmSuiteIdAlgAes256GcmHkdfSha512CommitKey
res, err := encryptionClient.Encrypt(context.Background(), esdktypes.EncryptInput{
    Plaintext:         []byte(exampleText),
    EncryptionContext: encryptionContext,
    Keyring:           aesKeyring,
    AlgorithmSuiteId:  &algorithmSuiteId,
})
if err != nil {
    panic(err)
}
```

Membatasi kunci data terenkripsi

Anda dapat membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Fitur praktik terbaik ini dapat membantu Anda mendeteksi keyring yang salah konfigurasi saat mengenkripsi atau ciphertext berbahaya saat mendekripsi. Ini juga mencegah panggilan yang tidak perlu, mahal, dan berpotensi lengkap ke infrastruktur utama Anda. Membatasi kunci data terenkripsi paling berharga saat Anda mendekripsi pesan dari sumber yang tidak tepercaya.

Meskipun sebagian besar pesan terenkripsi memiliki satu kunci data terenkripsi untuk setiap kunci pembungkus yang digunakan dalam enkripsi, pesan terenkripsi dapat berisi hingga 65.535 kunci data terenkripsi. Aktor jahat mungkin membuat pesan terenkripsi dengan ribuan kunci data terenkripsi, tidak ada yang dapat didekripsi. Akibatnya, AWS Encryption SDK akan mencoba untuk mendekripsi setiap kunci data terenkripsi sampai habis kunci data terenkripsi dalam pesan.

Untuk membatasi kunci data terenkripsi, gunakan parameter. `MaxEncryptedDataKeys` Parameter ini tersedia untuk semua bahasa pemrograman yang didukung mulai versi 1.9. x dan 2.2. x dari AWS Encryption SDK. Ini opsional dan valid saat mengenkripsi dan mendekripsi. Contoh berikut mendekripsi data yang dienkripsi di bawah tiga kunci pembungkus yang berbeda. `MaxEncryptedDataKeys`Nilai diatur ke 3.

C

```
/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();

/* Construct an AWS KMS keyring */
struct aws_cryptosdk_keyring *kms_keyring =
      Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn1, { key_arn2, key_arn3 });

/* Create a session */
struct aws_cryptosdk_session *session =
    aws_cryptosdk_session_new_from_keyring_2(alloc, AWS_CRYPTOSDK_DECRYPT,
 kms_keyring);
aws_cryptosdk_keyring_release(kms_keyring);

/* Limit encrypted data keys */
aws_cryptosdk_session_set_max_encrypted_data_keys(session, 3);

/* Decrypt */
size_t ciphertext_consumed_output;
aws_cryptosdk_session_process(session,
    plaintext_output,
    plaintext_buf_sz_output,
    &plaintext_len_output,
    ciphertext_input,
    ciphertext_len_input,
    &ciphertext_consumed_output);
assert(aws_cryptosdk_session_is_done(session));
assert(ciphertext_consumed == ciphertext_len);
```

C# / .NET

Untuk membatasi kunci data terenkripsi di AWS Encryption SDK for .NET, buat instance klien untuk.NET dan atur `MaxEncryptedDataKeys` parameter opsionalnya ke nilai yang diinginkan. AWS Encryption SDK Kemudian, panggil `Decrypt()` metode pada AWS Encryption SDK instance yang dikonfigurasi.

```
// Decrypt with limited data keys

// Instantiate the material providers
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders();
```

```
// Configure the commitment policy on the AWS Encryption SDK instance
var config = new AwsEncryptionSdkConfig
{
    MaxEncryptedDataKeys = 3
};
var encryptionSdk = AwsEncryptionSdkFactory.CreateAwsEncryptionSdk(config);

// Create the keyring
string keyArn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
var createKeyringInput = new CreateAwsKmsKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = keyArn
};
var decryptKeyring = materialProviders.CreateAwsKmsKeyring(createKeyringInput);

// Decrypt the ciphertext
var decryptInput = new DecryptInput
{
    Ciphertext = ciphertext,
    Keyring = decryptKeyring
};
var decryptOutput = encryptionSdk.Decrypt(decryptInput);
```

AWS Encryption CLI

```
# Decrypt with limited encrypted data keys

$ aws-encryption-cli --decrypt \
    --input hello.txt.encrypted \
    --wrapping-keys key=$key_arn1 key=$key_arn2 key=$key_arn3 \
    --buffer \
    --max-encrypted-data-keys 3 \
    --encryption-context purpose=test \
    --metadata-output ~/metadata \
    --output .
```

Java

```
// Construct a client with limited encrypted data keys
final AwsCrypto crypto = AwsCrypto.builder()
```

```
  .withMaxEncryptedDataKeys(3)
  .build();

// Create an AWS KMS master key provider
final KmsMasterKeyProvider keyProvider = KmsMasterKeyProvider.builder()
      .buildStrict(keyArn1, keyArn2, keyArn3);

// Decrypt
final CryptoResult<byte[], KmsMasterKey> decryptResult =
 crypto.decryptData(keyProvider, ciphertext)
```

JavaScript Browser

```
// Construct a client with limited encrypted data keys
const { encrypt, decrypt } = buildClient({ maxEncryptedDataKeys: 3 })

declare const credentials: {
  accessKeyId: string
  secretAccessKey: string
  sessionToken: string
}
const clientProvider = getClient(KMS, {
  credentials: { accessKeyId, secretAccessKey, sessionToken }
})

// Create an AWS KMS keyring
const keyring = new KmsKeyringBrowser({
  clientProvider,
  keyIds: [keyArn1, keyArn2, keyArn3],
})

// Decrypt
const { plaintext, messageHeader } = await decrypt(keyring, ciphertext)
```

JavaScript Node.js

```
// Construct a client with limited encrypted data keys
const { encrypt, decrypt } = buildClient({ maxEncryptedDataKeys: 3 })

// Create an AWS KMS keyring
const keyring = new KmsKeyringBrowser({
  keyIds: [keyArn1, keyArn2, keyArn3],
})
```

```
// Decrypt
const { plaintext, messageHeader } = await decrypt(keyring, ciphertext)
```

Python

```
# Instantiate a client with limited encrypted data keys
client = aws_encryption_sdk.EncryptionSDKClient(max_encrypted_data_keys=3)

# Create an AWS KMS master key provider
master_key_provider = aws_encryption_sdk.StrictAwsKmsMasterKeyProvider(
    key_ids=[key_arn1, key_arn2, key_arn3])

# Decrypt
plaintext, header = client.decrypt(source=ciphertext,
 key_provider=master_key_provider)
```

Rust

```
// Instantiate the AWS Encryption SDK client with limited encrypted data keys
let esdk_config = AwsEncryptionSdkConfig::builder()
                    .max_encrypted_data_keys(max_encrypted_data_keys)
                    .build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Define the key namespace and key name
let key_namespace: &str = "HSM_01";
let key_name: &str = "AES_256_012";

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

//  Generate `max_encrypted_data_keys` raw AES keyrings to use with your keyring
let mut raw_aes_keyrings: Vec<KeyringRef> = vec![];

assert!(max_encrypted_data_keys > 0, "max_encrypted_data_keys MUST be greater than
 0");

let mut i = 0;
while i < max_encrypted_data_keys {
    let aes_key_bytes = generate_aes_key_bytes();
```

```
    let raw_aes_keyring = mpl
        .create_raw_aes_keyring()
        .key_name(key_name)
        .key_namespace(key_namespace)
        .wrapping_key(aes_key_bytes)
        .wrapping_alg(AesWrappingAlg::AlgAes256GcmIv12Tag16)
        .send()
        .await?;

    raw_aes_keyrings.push(raw_aes_keyring);
    i += 1;
}

// Create a Multi Keyring with `max_encrypted_data_keys` AES Keyrings
let generator_keyring = raw_aes_keyrings.remove(0);

let multi_keyring = mpl
    .create_multi_keyring()
    .generator(generator_keyring)
    .child_keyrings(raw_aes_keyrings)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)

// Instantiate the AWS Encryption SDK client with limited encrypted data keys
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{
    MaxEncryptedDataKeys: &maxEncryptedDataKeys,
})
if err != nil {
```

```
    panic(err)
}

// Define the key namespace and key name
var keyNamespace = "HSM_01"
var keyName = "RSA_2048_06"

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

//  Generate `maxEncryptedDataKeys` raw AES keyrings to use with your keyring
rawAESKeyrings := make([]mpltypes.IKeyring, 0, maxEncryptedDataKeys)
var i int64 = 0
for i < maxEncryptedDataKeys {
    key, err := generate256KeyBytesAES()
 if err != nil {
  panic(err)
 }
    aesKeyRingInput := mpltypes.CreateRawAesKeyringInput{
  KeyName:      keyName,
  KeyNamespace: keyNamespace,
  WrappingKey:  key,
  WrappingAlg:  mpltypes.AesWrappingAlgAlgAes256GcmIv12Tag16,
 }
 aesKeyring, err := matProv.CreateRawAesKeyring(context.Background(),
 aesKeyRingInput)
    if err != nil {
  panic(err)
 }
    rawAESKeyrings = append(rawAESKeyrings, aesKeyring)
    i++
}

// Create a Multi Keyring with `max_encrypted_data_keys` AES Keyrings
createMultiKeyringInput := mpltypes.CreateMultiKeyringInput{
    Generator:     rawAESKeyrings[0],
    ChildKeyrings: rawAESKeyrings[1:],
}
multiKeyring, err := matProv.CreateMultiKeyring(context.Background(),
 createMultiKeyringInput)
if err != nil {
```

```
    panic(err)
}
```

Membuat filter penemuan

Saat mendekripsi data yang dienkripsi dengan kunci KMS, ini adalah praktik terbaik untuk mendekripsi dalam mode ketat, yaitu membatasi kunci pembungkus yang digunakan hanya untuk yang Anda tentukan. Namun, jika perlu, Anda juga dapat mendekripsi dalam mode penemuan, di mana Anda tidak menentukan kunci pembungkus apa pun. Dalam mode ini, AWS KMS dapat mendekripsi kunci data terenkripsi menggunakan kunci KMS yang mengenkripsi itu, terlepas dari siapa yang memiliki atau memiliki akses ke kunci KMS itu.

Jika Anda harus mendekripsi dalam mode penemuan, kami sarankan Anda selalu menggunakan filter penemuan, yang membatasi kunci KMS yang dapat digunakan untuk yang ada di partisi dan yang ditentukan Akun AWS . Filter penemuan adalah opsional, tetapi ini adalah praktik terbaik.

Gunakan tabel berikut untuk menentukan nilai partisi untuk filter penemuan Anda.

Region	Partition
Wilayah AWS	`aws`
Wilayah Tiongkok	`aws-cn`
AWS GovCloud (US) Regions	`aws-us-gov`

Contoh di bagian ini menunjukkan cara membuat filter penemuan. Sebelum menggunakan kode, ganti nilai contoh dengan nilai yang valid untuk partisi Akun AWS dan.

C

Untuk contoh lengkap, lihat kms_discovery.cpp di file AWS Encryption SDK for C.

```
/* Create a discovery filter for an AWS account and partition */

const char *account_id = "111122223333";
const char *partition = "aws";
const std::shared_ptr<Aws::Cryptosdk::KmsKeyring::DiscoveryFilter> discovery_filter
 =
```

```
 Aws::Cryptosdk::KmsKeyring::DiscoveryFilter::Builder(partition).AddAccount(account_id).Buil
```

C# / .NET

Untuk contoh lengkapnya, lihat DiscoveryFilterExample.cs di AWS Encryption SDK for .NET.

```
// Create a discovery filter for an AWS account and partition

List<string> account = new List<string> { "111122223333" };

DiscoveryFilter exampleDiscoveryFilter = new DiscoveryFilter()
{
    AccountIds = account,
    Partition = "aws"
}
```

AWS Encryption CLI

```
# Decrypt in discovery mode with a discovery filter

$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys discovery=true \
                                     discovery-account=111122223333 \
                                     discovery-partition=aws \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --max-encrypted-data-keys 1 \
                     --buffer \
                     --output .
```

Java

Untuk contoh lengkap, lihat DiscoveryDecryptionExample.java di file. AWS Encryption SDK for Java

```
// Create a discovery filter for an AWS account and partition

DiscoveryFilter discoveryFilter = new DiscoveryFilter("aws", 111122223333);
```

JavaScript (Node and Browser)

Untuk contoh lengkap, lihat kms_filtered_discovery.ts (Node.js) dan kms_multi_region_discovery.ts (Browser) di file. AWS Encryption SDK for JavaScript

```
/* Create a discovery filter for an AWS account and partition */
const discoveryFilter = {
  accountIDs: ['111122223333'],
  partition: 'aws',
}
```

Python

Untuk contoh lengkap, lihat discovery_kms_provider.py di file AWS Encryption SDK for Python.

```
# Create the discovery filter and specify the region
decrypt_kwargs = dict(
        discovery_filter=DiscoveryFilter(account_ids="111122223333",
 partition="aws"),
        discovery_region="us-west-2",
    )
```

Rust

```
let discovery_filter = DiscoveryFilter::builder()
    .account_ids(vec![111122223333.to_string()])
    .partition("aws".to_string())
    .build()?;
```

Go

```
import (
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
)

discoveryFilter := mpltypes.DiscoveryFilter{
    AccountIds: []string{111122223333},
    Partition:  "aws",
}
```

Mengkonfigurasi konteks enkripsi yang diperlukan CMM

Anda dapat menggunakan konteks enkripsi CMM yang diperlukan untuk memerlukan konteks enkripsi dalam operasi kriptografi Anda. Konteks enkripsi adalah sekumpulan pasangan kunci-nilai non-rahasia. Konteks enkripsi terikat secara kriptografis ke data terenkripsi sehingga konteks enkripsi yang sama diperlukan untuk mendekripsi bidang. Bila Anda menggunakan konteks enkripsi CMM yang diperlukan, Anda dapat menentukan satu atau beberapa kunci konteks enkripsi yang diperlukan (kunci wajib) yang harus disertakan dalam semua panggilan enkripsi dan dekripsi.

> **Note**
>
> Konteks enkripsi yang diperlukan CMM hanya didukung oleh versi berikut:
>
> - Versi 3. x dari AWS Encryption SDK for Java
> - Versi 4. x dari AWS Encryption SDK untuk .NET
> - Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.
> - Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go
>
> Jika Anda mengenkripsi data menggunakan konteks enkripsi CMM yang diperlukan, Anda hanya dapat mendekripsi dengan salah satu versi yang didukung ini.

Pada enkripsi, AWS Encryption SDK memverifikasi bahwa semua kunci konteks enkripsi yang diperlukan disertakan dalam konteks enkripsi yang Anda tentukan. AWS Encryption SDK Tanda konteks enkripsi yang Anda tentukan. Hanya pasangan kunci-nilai yang bukan kunci wajib yang diserialisasi dan disimpan dalam teks biasa di header pesan terenkripsi yang dikembalikan oleh operasi enkripsi.

Saat mendekripsi, Anda harus menyediakan konteks enkripsi yang berisi semua pasangan kunci-nilai yang mewakili kunci yang diperlukan. AWS Encryption SDK Menggunakan konteks enkripsi ini dan pasangan kunci-nilai yang disimpan dalam header pesan terenkripsi untuk merekonstruksi konteks enkripsi asli yang Anda tentukan dalam operasi enkripsi. Jika AWS Encryption SDK tidak dapat merekonstruksi konteks enkripsi asli, maka operasi dekripsi gagal. Jika Anda memberikan pasangan kunci-nilai yang berisi kunci yang diperlukan dengan nilai yang salah, pesan terenkripsi tidak dapat didekripsi. Anda harus memberikan pasangan nilai kunci yang sama yang ditentukan pada enkripsi.

> **Important**
>
> Pertimbangkan dengan cermat nilai mana yang Anda pilih untuk kunci yang diperlukan dalam konteks enkripsi Anda. Anda harus dapat memberikan kunci yang sama dan nilai yang sesuai lagi pada dekripsi. Jika Anda tidak dapat mereproduksi kunci yang diperlukan, pesan terenkripsi tidak dapat didekripsi.

Contoh berikut menginisialisasi AWS KMS keyring dengan konteks enkripsi CMM yang diperlukan.

C# / .NET

```
var encryptionContext = new Dictionary<string, string>()
{
    {"encryption", "context"},
    {"is not", "secret"},
    {"but adds", "useful metadata"},
    {"that can help you", "be confident that"},
    {"the data you are handling", "is what you think it is"}
};

// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

// Instantiate the keyring input object
var createKeyringInput = new CreateAwsKmsKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = kmsKey
};

// Create the keyring
var kmsKeyring = mpl.CreateAwsKmsKeyring(createKeyringInput);

var createCMMInput = new CreateRequiredEncryptionContextCMMInput
{
    UnderlyingCMM = mpl.CreateDefaultCryptographicMaterialsManager(new
 CreateDefaultCryptographicMaterialsManagerInput{Keyring = kmsKeyring}),
    // If you pass in a keyring but no underlying cmm, it will result in a failure
 because only cmm is supported.
    RequiredEncryptionContextKeys = new List<string>(encryptionContext.Keys)
```

```
};

// Create the required encryption context CMM
var requiredEcCMM = mpl.CreateRequiredEncryptionContextCMM(createCMMInput);
```

Java

```
// Instantiate the AWS Encryption SDK
final AwsCrypto crypto = AwsCrypto.builder()
        .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
        .build();

// Create your encryption context
final Map<String, String> encryptionContext = new HashMap<>();
encryptionContext.put("encryption", "context");
encryptionContext.put("is not", "secret");
encryptionContext.put("but adds", "useful metadata");
encryptionContext.put("that can help you", "be confident that");
encryptionContext.put("the data you are handling", "is what you think it is");

// Create a list of required encryption contexts
final List<String> requiredEncryptionContextKeys = Arrays.asList("encryption",
 "context");

// Create the keyring
final MaterialProviders materialProviders = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();
final CreateAwsKmsKeyringInput keyringInput = CreateAwsKmsKeyringInput.builder()
        .kmsKeyId(keyArn)
        .kmsClient(KmsClient.create())
        .build();
IKeyring kmsKeyring = materialProviders.CreateAwsKmsKeyring(keyringInput);

// Create the required encryption context CMM
ICryptographicMaterialsManager cmm =
    materialProviders.CreateDefaultCryptographicMaterialsManager(
        CreateDefaultCryptographicMaterialsManagerInput.builder()
            .keyring(kmsKeyring)
            .build()
    );
ICryptographicMaterialsManager requiredCMM =
    materialProviders.CreateRequiredEncryptionContextCMM(
```

```
        CreateRequiredEncryptionContextCMMInput.builder()
            .requiredEncryptionContextKeys(requiredEncryptionContextKeys)
            .underlyingCMM(cmm)
            .build()
        );
```

Python

Untuk menggunakan CMM konteks enkripsi yang diperlukan, Anda juga harus menggunakan pustaka penyedia materi (MPL). AWS Encryption SDK for Python

```
# Instantiate the AWS Encryption SDK client
client = aws_encryption_sdk.EncryptionSDKClient(
    commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

# Create your encryption context
encryption_context: Dict[str, str] = {
    "key1": "value1",
    "key2": "value2",
    "requiredKey1": "requiredValue1",
    "requiredKey2": "requiredValue2"
}

# Create a list of required encryption context keys
required_encryption_context_keys: List[str] = ["requiredKey1", "requiredKey2"]

# Instantiate the material providers library
mpl: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create the AWS KMS keyring
 keyring_input: CreateAwsKmsKeyringInput = CreateAwsKmsKeyringInput(
    kms_key_id=kms_key_id,
    kms_client=boto3.client('kms', region_name="us-west-2")
)
kms_keyring: IKeyring = mpl.create_aws_kms_keyring(keyring_input)

# Create the required encryption context CMM
underlying_cmm: ICryptographicMaterialsManager = \
    mpl.create_default_cryptographic_materials_manager(
        CreateDefaultCryptographicMaterialsManagerInput(
```

```
            keyring=kms_keyring
        )
    )

required_ec_cmm: ICryptographicMaterialsManager = \
    mpl.create_required_encryption_context_cmm(
        CreateRequiredEncryptionContextCMMInput(
            required_encryption_context_keys=required_encryption_context_keys,
            underlying_cmm=underlying_cmm,
        )
    )
```

Rust

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create an AWS KMS client
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Create your encryption context
let encryption_context = HashMap::from([
    ("key1".to_string(), "value1".to_string()),
    ("key2".to_string(), "value2".to_string()),
    ("requiredKey1".to_string(), "requiredValue1".to_string()),
    ("requiredKey2".to_string(), "requiredValue2".to_string()),
]);

// Create a list of required encryption context keys
let required_encryption_context_keys: Vec<String> = vec![
    "requiredKey1".to_string(),
    "requiredKey2".to_string(),
];

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create the AWS KMS keyring
let kms_keyring = mpl
```

```
    .create_aws_kms_keyring()
    .kms_key_id(kms_key_id)
    .kms_client(kms_client)
    .send()
    .await?;

kms_multi_keyring: IKeyring = mat_prov.create_aws_kms_multi_keyring(
    input=kms_multi_keyring_input
)

// Create the required encryption context CMM
let underlying_cmm = mpl
    .create_default_cryptographic_materials_manager()
    .keyring(kms_keyring)
    .send()
    .await?;

let required_ec_cmm = mpl
    .create_required_encryption_context_cmm()
    .underlying_cmm(underlying_cmm.clone())
    .required_encryption_context_keys(required_encryption_context_keys)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
```

```
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = defaultKmsKeyRegion
})

// Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Create a list of required encryption context keys
requiredEncryptionContextKeys := []string{}
requiredEncryptionContextKeys = append(requiredEncryptionContextKeys,
 "requiredKey1", "requiredKey2")

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create the AWS KMS keyring
awsKmsKeyringInput := mpltypes.CreateAwsKmsKeyringInput{
    KmsClient: kmsClient,
    KmsKeyId:  utils.GetDefaultKMSKeyId(),
}
awsKmsKeyring, err := matProv.CreateAwsKmsKeyring(context.Background(),
 awsKmsKeyringInput)
if err != nil {
    panic(err)
}
```

```
// Create the required encryption context CMM
underlyingCMM, err :=
 matProv.CreateDefaultCryptographicMaterialsManager(context.Background(),
 mpltypes.CreateDefaultCryptographicMaterialsManagerInput{Keyring: awsKmsKeyring})
if err != nil {
    panic(err)
}
requiredEncryptionContextInput := mpltypes.CreateRequiredEncryptionContextCMMInput{
    UnderlyingCMM: underlyingCMM,
    RequiredEncryptionContextKeys: requiredEncryptionContextKeys,
}
requiredEC, err := matProv.CreateRequiredEncryptionContextCMM(context.Background(),
 requiredEncryptionContextInput)
if err != nil {
    panic(err)
}
```

Menetapkan kebijakan komitmen

Kebijakan komitmen adalah pengaturan konfigurasi yang menentukan apakah aplikasi Anda mengenkripsi dan mendekripsi dengan komitmen utama. Mengenkripsi dan mendekripsi dengan komitmen utama adalah praktik terbaik.AWS Encryption SDK

Menyetel dan menyesuaikan kebijakan komitmen Anda adalah langkah penting dalam bermigrasi dari versi 1.7. x dan sebelumnya AWS Encryption SDK ke versi 2.0. x dan kemudian. Perkembangan ini dijelaskan secara rinci dalam topik migrasi.

Nilai kebijakan komitmen default di versi terbaru AWS Encryption SDK (dimulai pada versi 2.0. x),`RequireEncryptRequireDecrypt`, sangat ideal untuk sebagian besar situasi. Namun, jika Anda perlu mendekripsi ciphertext yang dienkripsi tanpa komitmen utama, Anda mungkin perlu mengubah kebijakan komitmen Anda. `RequireEncryptAllowDecrypt` Untuk contoh cara menetapkan kebijakan komitmen dalam setiap bahasa pemrograman, lihatMenetapkan kebijakan komitmen Anda.

Bekerja dengan data streaming

Saat Anda mengalirkan data untuk dekripsi, ketahuilah bahwa teks biasa yang didekripsi AWS Encryption SDK kembali setelah pemeriksaan integritas selesai, tetapi sebelum tanda tangan digital

diverifikasi. Untuk memastikan bahwa Anda tidak mengembalikan atau menggunakan plaintext sampai tanda tangan diverifikasi, kami sarankan Anda menyangga plaintext yang dialirkan hingga seluruh proses dekripsi selesai.

Masalah ini muncul hanya ketika Anda melakukan streaming ciphertext untuk dekripsi, dan hanya ketika Anda menggunakan rangkaian algoritme, seperti rangkaian algoritme default, yang menyertakan tanda tangan digital.

Untuk mempermudah buffering, beberapa implementasi AWS Encryption SDK bahasa, seperti AWS Encryption SDK for JavaScript di Node.js, menyertakan fitur buffering sebagai bagian dari metode dekripsi. AWS Encryption CLI, yang selalu mengalirkan input dan output memperkenalkan `--buffer` parameter dalam versi 1.9. x dan 2.2. x. Dalam implementasi bahasa lain, Anda dapat menggunakan fitur buffering yang ada. (AWS Encryption SDK Untuk .NET tidak mendukung streaming.)

Jika Anda menggunakan rangkaian algoritme tanpa tanda tangan digital, pastikan untuk menggunakan `decrypt-unsigned` fitur ini di setiap implementasi bahasa. Fitur ini mendekripsi ciphertext tetapi gagal jika menemukan ciphertext yang ditandatangani. Lihat perinciannya di Memilih rangkaian algoritme.

Menyembunyikan kunci data

Secara umum, menggunakan kembali kunci data tidak disarankan, tetapi AWS Encryption SDK menawarkan opsi caching kunci data yang menyediakan penggunaan kembali kunci data secara terbatas. Caching kunci data dapat meningkatkan kinerja beberapa aplikasi dan mengurangi panggilan ke infrastruktur utama Anda. Sebelum menggunakan caching kunci data dalam produksi, sesuaikan ambang keamanan, dan uji untuk memastikan bahwa manfaatnya lebih besar daripada kerugian menggunakan kembali kunci data.

Toko-toko utama di AWS Encryption SDK

Dalam AWS Encryption SDK, penyimpanan kunci adalah tabel Amazon DynamoDB yang mempertahankan data hierarkis yang digunakan oleh keyring Hierarkis.AWS KMS Toko kunci membantu mengurangi jumlah panggilan yang perlu Anda lakukan AWS KMS untuk melakukan operasi kriptografi dengan keyring Hierarkis.

Penyimpanan kunci tetap ada dan mengelola kunci cabang yang digunakan keyring Hierarkis untuk melakukan enkripsi amplop dan melindungi kunci enkripsi data. Key store menyimpan kunci cabang aktif dan semua versi sebelumnya dari kunci cabang. Kunci cabang aktif adalah versi kunci cabang terbaru. Keyring Hierarkis menggunakan kunci enkripsi data unik untuk setiap permintaan enkripsi dan mengenkripsi setiap kunci enkripsi data dengan kunci pembungkus unik yang berasal dari kunci cabang aktif. Keyring Hierarkis tergantung pada hierarki yang ditetapkan antara kunci cabang aktif dan kunci pembungkus turunannya.

Terminologi dan konsep toko kunci

Toko kunci

Tabel DynamoDB yang mempertahankan data hierarkis, seperti kunci cabang dan kunci suar.

Kunci root

Kunci KMS enkripsi simetris yang menghasilkan dan melindungi kunci cabang dan kunci suar di toko kunci Anda.

Kunci cabang

Kunci data yang digunakan kembali untuk mendapatkan kunci pembungkus unik untuk enkripsi amplop. Anda dapat membuat beberapa kunci cabang dalam satu penyimpanan kunci, tetapi setiap kunci cabang hanya dapat memiliki satu versi kunci cabang aktif pada satu waktu. Kunci cabang aktif adalah versi kunci cabang terbaru.

Kunci cabang berasal dari AWS KMS keys menggunakan kms: GenerateDataKeyWithoutPlaintext operasi.

Kunci pembungkus

Kunci data unik yang digunakan untuk mengenkripsi kunci enkripsi data yang digunakan dalam operasi enkripsi.

Kunci pembungkus berasal dari kunci cabang. Untuk informasi selengkapnya tentang proses derivasi kunci, lihat Detail teknis keyring AWS KMS hierarkis.

Kunci enkripsi data

Kunci data yang digunakan dalam operasi enkripsi. Keyring Hierarkis menggunakan kunci enkripsi data unik untuk setiap permintaan enkripsi.

Menerapkan izin yang paling tidak diistimewakan

Saat menggunakan penyimpanan kunci dan gantungan kunci AWS KMS Hierarkis, kami sarankan Anda mengikuti prinsip hak istimewa paling sedikit dengan mendefinisikan peran berikut:

Administrator toko kunci

Administrator toko utama bertanggung jawab untuk membuat dan mengelola toko kunci dan kunci cabang yang bertahan dan dilindungi. Administrator toko utama harus menjadi satu-satunya pengguna dengan izin menulis ke tabel Amazon DynamoDB yang berfungsi sebagai toko kunci Anda. Mereka harus menjadi satu-satunya pengguna dengan akses ke operasi administrator istimewa, seperti `CreateKey`dan `VersionKey`. Anda hanya dapat melakukan operasi ini ketika Anda mengonfigurasi tindakan penyimpanan kunci secara statis.

`CreateKey`adalah operasi istimewa yang dapat menambahkan ARN kunci KMS baru ke daftar izin toko kunci Anda. Kunci KMS ini dapat membuat kunci cabang aktif baru. Kami menyarankan untuk membatasi akses ke operasi ini karena setelah kunci KMS ditambahkan ke toko kunci cabang, itu tidak dapat dihapus.

Pengguna toko kunci

Dalam kebanyakan kasus penggunaan, pengguna key store hanya berinteraksi dengan key store melalui keyring Hierarchical saat mereka mengenkripsi, mendekripsi, menandatangani, dan memverifikasi data. Akibatnya, mereka hanya perlu izin baca ke tabel Amazon DynamoDB yang berfungsi sebagai toko kunci Anda. Pengguna toko kunci hanya perlu akses ke operasi penggunaan yang memungkinkan operasi kriptografi, seperti`GetActiveBranchKey`,`GetBranchKeyVersion`, dan`GetBeaconKey`. Mereka tidak memerlukan izin untuk membuat atau mengelola kunci cabang yang mereka gunakan.

Anda dapat melakukan operasi penggunaan ketika tindakan penyimpanan kunci Anda dikonfigurasi secara statis, atau ketika mereka dikonfigurasi untuk penemuan. Anda tidak dapat

melakukan operasi administrator (`CreateKeydanVersionKey`) ketika tindakan penyimpanan kunci Anda dikonfigurasi untuk penemuan.

Jika administrator toko kunci cabang Anda mengizinkan daftar beberapa kunci KMS di toko kunci cabang Anda, kami menyarankan agar pengguna toko kunci Anda mengonfigurasi tindakan penyimpanan kunci mereka untuk ditemukan sehingga keyring Hierarkis mereka dapat menggunakan beberapa kunci KMS.

Buat toko kunci

Sebelum Anda dapat membuat kunci cabang atau menggunakan keyring AWS KMS Hierarkis, Anda harus membuat toko kunci Anda, tabel Amazon DynamoDB yang mengelola dan melindungi kunci cabang Anda.

> **Important**
>
> Jangan hapus tabel DynamoDB yang mempertahankan kunci cabang Anda. Jika Anda menghapus tabel ini, Anda tidak akan dapat mendekripsi data apa pun yang dienkripsi menggunakan keyring Hierarkis.

Ikuti prosedur Buat tabel di Panduan Pengembang Amazon DynamoDB, menggunakan nilai string yang diperlukan berikut untuk kunci partisi dan kunci sortir.

	Kunci partisi	Sortir kunci
Tabel dasar	`branch-key-id`	`type`

Nama toko kunci logis

Saat menamai tabel DynamoDB yang berfungsi sebagai penyimpanan kunci Anda, penting untuk mempertimbangkan dengan cermat nama toko kunci logis yang akan Anda tentukan saat mengonfigurasi tindakan penyimpanan kunci Anda. Nama penyimpanan kunci logis bertindak sebagai pengidentifikasi untuk toko kunci Anda dan tidak dapat diubah setelah awalnya ditentukan oleh pengguna pertama. Anda harus selalu menentukan nama penyimpanan kunci logis yang sama dalam tindakan penyimpanan kunci Anda.

Harus ada one-to-one pemetaan antara nama tabel DynamoDB dan nama toko kunci logis. Nama penyimpanan kunci logis terikat secara kriptografis ke semua data yang disimpan dalam tabel untuk menyederhanakan operasi pemulihan DynamoDB. Meskipun nama toko kunci logis dapat berbeda dari nama tabel DynamoDB Anda, kami sangat menyarankan untuk menentukan nama tabel DynamoDB Anda sebagai nama toko kunci logis. Jika nama tabel Anda berubah setelah memulihkan tabel DynamoDB Anda dari cadangan, nama penyimpanan kunci logis dapat dipetakan ke nama tabel DynamoDB baru untuk memastikan bahwa keyring Hierarkis masih dapat mengakses penyimpanan kunci Anda.

Jangan sertakan informasi rahasia atau sensitif dalam nama toko kunci logis Anda. Nama penyimpanan kunci logis ditampilkan dalam teks biasa dalam AWS KMS CloudTrail peristiwa sebagai. `tablename`

Langkah selanjutnya

1. the section called “Konfigurasikan tindakan penyimpanan kunci”
2. the section called “Buat kunci cabang”
3. Buat keyring AWS KMS Hierarkis

Konfigurasikan tindakan penyimpanan kunci

Tindakan penyimpanan kunci menentukan operasi apa yang dapat dilakukan pengguna Anda dan bagaimana keyring AWS KMS Hierarkis mereka menggunakan kunci KMS yang diizinkan terdaftar di toko kunci Anda. AWS Encryption SDK Mendukung konfigurasi tindakan penyimpanan kunci berikut.

Statis

Saat Anda mengonfigurasi penyimpanan kunci secara statis, toko kunci hanya dapat menggunakan kunci KMS yang terkait dengan ARN kunci KMS yang Anda berikan `kmsConfiguration` saat Anda mengonfigurasi tindakan penyimpanan kunci Anda. Pengecualian dilemparkan jika ARN kunci KMS yang berbeda ditemukan saat membuat, membuat versi, atau mendapatkan kunci cabang.

Anda dapat menentukan kunci KMS Multi-wilayah di Anda`kmsConfiguration`, tetapi seluruh ARN kunci, termasuk wilayah, disimpan di kunci cabang yang berasal dari kunci KMS. Anda tidak dapat menentukan kunci di wilayah yang berbeda, Anda harus memberikan kunci multi-wilayah yang sama persis agar nilainya cocok.

Saat Anda mengonfigurasi tindakan penyimpanan kunci secara statis, Anda dapat melakukan operasi penggunaan (`GetActiveBranchKey`,`GetBranchKeyVersion`,`GetBeaconKey`) dan operasi administratif (`CreateKey`dan`VersionKey`). `CreateKey`adalah operasi istimewa yang dapat menambahkan ARN kunci KMS baru ke daftar izin toko kunci Anda. Kunci KMS ini dapat membuat kunci cabang aktif baru. Kami menyarankan untuk membatasi akses ke operasi ini karena setelah kunci KMS ditambahkan ke toko kunci, itu tidak dapat dihapus.

Penemuan

Saat Anda mengonfigurasi tindakan penyimpanan kunci untuk penemuan, toko kunci dapat menggunakan AWS KMS key ARN apa pun yang diizinkan terdaftar di toko kunci Anda. Namun, pengecualian dilemparkan ketika kunci KMS Multi-wilayah ditemui dan wilayah di ARN kunci tidak cocok dengan wilayah klien yang digunakan. AWS KMS

Ketika Anda mengonfigurasi penyimpanan kunci untuk penemuan, Anda tidak dapat melakukan operasi administratif, seperti `CreateKey` dan`VersionKey`. Anda hanya dapat melakukan operasi penggunaan yang mengaktifkan enkripsi, mendekripsi, menandatangani, dan memverifikasi operasi. Untuk informasi selengkapnya, lihat the section called “Menerapkan izin yang paling tidak diistimewakan”.

Konfigurasikan tindakan penyimpanan kunci Anda

Sebelum Anda mengonfigurasi tindakan penyimpanan kunci Anda, pastikan prasyarat berikut terpenuhi.

- Tentukan operasi apa yang perlu Anda lakukan. Untuk informasi selengkapnya, lihat the section called “Menerapkan izin yang paling tidak diistimewakan”.
- Pilih nama toko kunci logis

  Harus ada one-to-one pemetaan antara nama tabel DynamoDB dan nama toko kunci logis. Nama penyimpanan kunci logis terikat secara kriptografis ke semua data yang disimpan dalam tabel untuk menyederhanakan operasi pemulihan DynamoDB, tidak dapat diubah setelah awalnya ditentukan oleh pengguna pertama. Anda harus selalu menentukan nama penyimpanan kunci logis yang sama dalam tindakan penyimpanan kunci Anda. Untuk informasi selengkapnya, lihat logical key store name.

Konfigurasi statis

Contoh berikut secara statis mengkonfigurasi tindakan penyimpanan kunci. Anda harus menentukan nama tabel DynamoDB yang berfungsi sebagai penyimpanan kunci Anda, nama logis untuk penyimpanan kunci, dan ARN kunci KMS yang mengidentifikasi kunci KMS enkripsi simetris.

> **Note**
>
> Pertimbangkan dengan cermat ARN kunci KMS yang Anda tentukan saat mengonfigurasi layanan penyimpanan kunci Anda secara statis. `CreateKey`Operasi menambahkan ARN kunci KMS ke daftar izin toko kunci cabang Anda. Setelah kunci KMS ditambahkan ke toko kunci cabang, itu tidak dapat dihapus.

Java

```
final KeyStore keystore = KeyStore.builder().KeyStoreConfig(
                  KeyStoreConfig.builder()
                          .ddbClient(DynamoDbClient.create())
                          .ddbTableName(keyStoreName)
                          .logicalKeyStoreName(logicalKeyStoreName)
                          .kmsClient(KmsClient.create())
                          .kmsConfiguration(KMSConfiguration.builder()
                                  .kmsKeyArn(kmsKeyArn)
                                  .build())
                          .build()).build();
```

C# / .NET

```
var kmsConfig = new KMSConfiguration { KmsKeyArn = kmsKeyArn };
  var keystoreConfig = new KeyStoreConfig
  {
      KmsClient = new AmazonKeyManagementServiceClient(),
      KmsConfiguration = kmsConfig,
      DdbTableName = keyStoreName,
      DdbClient = new AmazonDynamoDBClient(),
      LogicalKeyStoreName = logicalKeyStoreName
  };
  var keystore = new KeyStore(keystoreConfig);
```

Python

```
keystore: KeyStore = KeyStore(
    config=KeyStoreConfig(
        ddb_client=ddb_client,
        ddb_table_name=key_store_name,
        logical_key_store_name=logical_key_store_name,
        kms_client=kms_client,
        kms_configuration=KMSConfigurationKmsKeyArn(
            value=kms_key_id
        ),
    )
)
```

Rust

```
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let key_store_config = KeyStoreConfig::builder()
    .kms_client(aws_sdk_kms::Client::new(&sdk_config))
    .ddb_client(aws_sdk_dynamodb::Client::new(&sdk_config))
    .ddb_table_name(key_store_name)
    .logical_key_store_name(logical_key_store_name)
    .kms_configuration(KmsConfiguration::KmsKeyArn(kms_key_arn.to_string()))
    .build()?;

let keystore = keystore_client::Client::from_conf(key_store_config)?;
```

Go

```
import (
 keystore "github.com/aws/aws-cryptographic-material-providers-library/mpl/
awscryptographykeystoresmithygenerated"
 keystoretypes "github.com/aws/aws-cryptographic-material-providers-library/mpl/
awscryptographykeystoresmithygeneratedtypes"
)

kmsConfig := keystoretypes.KMSConfigurationMemberkmsKeyArn{
    Value: kmsKeyArn,
}
keyStore, err := keystore.NewClient(keystoretypes.KeyStoreConfig{
    DdbTableName:        keyStoreTableName,
    KmsConfiguration:    &kmsConfig,
```

```
    LogicalKeyStoreName: logicalKeyStoreName,
    DdbClient:           ddbClient,
    KmsClient:           kmsClient,
})
if err != nil {
    panic(err)
}
```

Konfigurasi penemuan

Contoh berikut mengonfigurasi tindakan penyimpanan kunci untuk penemuan. Anda harus menentukan nama tabel DynamoDB yang berfungsi sebagai toko kunci Anda dan nama toko kunci logis.

Java

```
final KeyStore keystore = KeyStore.builder().KeyStoreConfig(
                KeyStoreConfig.builder()
                        .ddbClient(DynamoDbClient.create())
                        .ddbTableName(keyStoreName)
                        .logicalKeyStoreName(logicalKeyStoreName)
                        .kmsClient(KmsClient.create())
                        .kmsConfiguration(KMSConfiguration.builder()
                                .discovery(Discovery.builder().build())
                                .build())
                        .build()).build();
```

C# / .NET

```
var keystoreConfig = new KeyStoreConfig
 {
     KmsClient = new AmazonKeyManagementServiceClient(),
     KmsConfiguration = new KMSConfiguration {Discovery = new Discovery()},
     DdbTableName = keyStoreName,
     DdbClient = new AmazonDynamoDBClient(),
     LogicalKeyStoreName = logicalKeyStoreName
 };
 var keystore = new KeyStore(keystoreConfig);
```

Python

```
keystore: KeyStore = KeyStore(
    config=KeyStoreConfig(
        ddb_client=ddb_client,
        ddb_table_name=key_store_name,
        logical_key_store_name=logical_key_store_name,
        kms_client=kms_client,
        kms_configuration=KMSConfigurationDiscovery(
            value=Discovery()
        ),
    )
)
```

Rust

```
let key_store_config = KeyStoreConfig::builder()
        .kms_client(kms_client)
        .ddb_client(ddb_client)
        .ddb_table_name(key_store_name)
        .logical_key_store_name(logical_key_store_name)

 .kms_configuration(KmsConfiguration::Discovery(Discovery::builder().build()?))
        .build()?;
```

Go

```
import (
 keystore "github.com/aws/aws-cryptographic-material-providers-library/mpl/
awscryptographykeystoresmithygenerated"
 keystoretypes "github.com/aws/aws-cryptographic-material-providers-library/mpl/
awscryptographykeystoresmithygeneratedtypes"
)

kmsConfig := keystoretypes.KMSConfigurationMemberdiscovery{}
keyStore, err := keystore.NewClient(keystoretypes.KeyStoreConfig{
    DdbTableName:        keyStoreName,
    KmsConfiguration:    &kmsConfig,
    LogicalKeyStoreName: logicalKeyStoreName,
    DdbClient:           ddbClient,
    KmsClient:           kmsClient,
})
if err != nil {
```

```
    panic(err)
}
```

Buat kunci cabang aktif

Kunci cabang adalah kunci data yang berasal dari AWS KMS key yang digunakan oleh keyring AWS KMS Hierarkis untuk mengurangi jumlah panggilan yang dilakukan. AWS KMS Kunci cabang aktif adalah versi kunci cabang terbaru. Keyring Hierarkis menghasilkan kunci data unik untuk setiap permintaan enkripsi dan mengenkripsi setiap kunci data dengan kunci pembungkus unik yang berasal dari kunci cabang aktif.

Untuk membuat kunci cabang aktif baru, Anda harus mengonfigurasi tindakan penyimpanan kunci secara statis. `CreateKey`adalah operasi istimewa yang menambahkan ARN kunci KMS yang ditentukan dalam konfigurasi tindakan penyimpanan kunci Anda ke daftar izin toko kunci Anda. Kemudian, kunci KMS digunakan untuk menghasilkan kunci cabang aktif baru. Kami menyarankan untuk membatasi akses ke operasi ini karena setelah kunci KMS ditambahkan ke toko kunci, itu tidak dapat dihapus.

Anda dapat mengizinkan daftar satu kunci KMS di toko kunci Anda, atau Anda dapat mengizinkan beberapa kunci KMS dengan memperbarui ARN kunci KMS yang Anda tentukan dalam konfigurasi tindakan penyimpanan kunci Anda dan menelepon lagi. `CreateKey` Jika Anda mengizinkan beberapa kunci KMS, pengguna toko kunci Anda harus mengonfigurasi tindakan penyimpanan kunci mereka untuk penemuan sehingga mereka dapat menggunakan salah satu kunci yang diizinkan di toko kunci yang dapat mereka akses. Untuk informasi selengkapnya, lihat the section called “Konfigurasikan tindakan penyimpanan kunci”.

Izin yang diperlukan

Untuk membuat kunci cabang, Anda memerlukan ReEncrypt izin kms: GenerateDataKeyWithoutPlaintext dan kms: pada kunci KMS yang ditentukan dalam tindakan penyimpanan kunci Anda.

Buat kunci cabang

Operasi berikut membuat kunci cabang aktif baru menggunakan kunci KMS yang Anda tentukan dalam konfigurasi tindakan penyimpanan kunci Anda, dan menambahkan kunci cabang aktif ke tabel DynamoDB yang berfungsi sebagai penyimpanan kunci Anda.

Saat Anda meneleponCreateKey, Anda dapat memilih untuk menentukan nilai opsional berikut.

- `branchKeyIdentifier`: mendefinisikan kustom`branch-key-id`.

  Untuk membuat kustom`branch-key-id`, Anda juga harus menyertakan konteks enkripsi tambahan dengan `encryptionContext` parameter.

- `encryptionContext`: mendefinisikan kumpulan opsional pasangan kunci-nilai non-rahasia yang menyediakan data terautentikasi tambahan (AAD) dalam konteks enkripsi yang disertakan dalam panggilan kms:. GenerateDataKeyWithoutPlaintext

  Konteks enkripsi tambahan ini ditampilkan dengan `aws-crypto-ec:` awalan.

Java

```
final Map<String, String> additionalEncryptionContext =
 Collections.singletonMap("Additional Encryption Context for",
         "custom branch key id");

  final String BranchKey = keystore.CreateKey(
         CreateKeyInput.builder()
                 .branchKeyIdentifier(custom-branch-key-id) //OPTIONAL
                 .encryptionContext(additionalEncryptionContext) //OPTIONAL

                 .build()).branchKeyIdentifier();
```

C# / .NET

```
var additionalEncryptionContext = new Dictionary<string, string>();
  additionalEncryptionContext.Add("Additional Encryption Context for", "custom
 branch key id");

  var branchKeyId = keystore.CreateKey(new CreateKeyInput
  {
      BranchKeyIdentifier = "custom-branch-key-id", // OPTIONAL
      EncryptionContext = additionalEncryptionContext // OPTIONAL
  });
```

Python

```
additional_encryption_context = {"Additional Encryption Context for": "custom branch
 key id"}

branch_key_id: str = keystore.create_key(
```

```
    CreateKeyInput(
        branch_key_identifier = "custom-branch-key-id", # OPTIONAL
        encryption_context = additional_encryption_context, # OPTIONAL
    )
)
```

Rust

```
let additional_encryption_context = HashMap::from([
    ("Additional Encryption Context for".to_string(), "custom branch key
 id".to_string())
]);

let branch_key_id = keystore.create_key()
    .branch_key_identifier("custom-branch-key-id") // OPTIONAL
    .encryption_context(additional_encryption_context) // OPTIONAL
    .send()
    .await?
    .branch_key_identifier
    .unwrap();
```

Go

```
encryptionContext := map[string]string{
    "Additional Encryption Context for": "custom branch key id",
}

branchKey, err := keyStore.CreateKey(context.Background(),
 keystoretypes.CreateKeyInput{
    BranchKeyIdentifier: &customBranchKeyId,
    EncryptionContext:   additional_encryption_context,
})
if err != nil {
    return "", err
}
```

Pertama, `CreateKey` operasi menghasilkan nilai-nilai berikut.

- Versi 4 Universally Unique Identifier (UUID) untuk `branch-key-id` (kecuali Anda menentukan kustom). `branch-key-id`
- UUID versi 4 untuk versi kunci cabang

- A `timestamp` dalam format tanggal dan waktu ISO 8601 dalam Coordinated Universal Time (UTC).

Kemudian, `CreateKey` operasi memanggil kms: GenerateDataKeyWithoutPlaintext menggunakan permintaan berikut.

```
{
     "EncryptionContext": {
        "branch-key-id" : "branch-key-id",
        "type" : "type",
        "create-time" : "timestamp",
        "logical-key-store-name" : "the logical table name for your key store",
        "kms-arn" : the KMS key ARN,
        "hierarchy-version" : "1",
        "aws-crypto-ec:contextKey": "contextValue"
     },
     "KeyId": "the KMS key ARN you specified in your key store actions",
     "NumberOfBytes": "32"
  }
```

Selanjutnya, `CreateKey` operasi memanggil kms: ReEncrypt untuk membuat catatan aktif untuk kunci cabang dengan memperbarui konteks enkripsi.

Terakhir, `CreateKey` operasi memanggil ddb: TransactWriteItems untuk menulis item baru yang akan mempertahankan kunci cabang dalam tabel yang Anda buat di Langkah 2. Item memiliki atribut berikut.

```
{
      "branch-key-id" : branch-key-id,
      "type" : "branch:ACTIVE",
      "enc" : the branch key returned by the GenerateDataKeyWithoutPlaintext call,
      "version": "branch:version:the branch key version UUID",
      "create-time" : "timestamp",
      "kms-arn" : "the KMS key ARN you specified in Step 1",
      "hierarchy-version" : "1",
      "aws-crypto-ec:contextKey": "contextValue"
 }
```

Putar kunci cabang aktif Anda

Hanya ada satu versi aktif untuk setiap kunci cabang pada satu waktu. Biasanya, setiap versi kunci cabang aktif digunakan untuk memenuhi beberapa permintaan. Tetapi Anda mengontrol sejauh mana kunci cabang aktif digunakan kembali dan menentukan seberapa sering kunci cabang aktif diputar.

Kunci cabang tidak digunakan untuk mengenkripsi kunci data teks biasa. Mereka digunakan untuk mendapatkan kunci pembungkus unik yang mengenkripsi kunci data teks biasa. Proses derivasi kunci pembungkus menghasilkan kunci pembungkus 32 byte yang unik dengan 28 byte keacakan. Ini berarti bahwa kunci cabang dapat memperoleh lebih dari 79 oktillion, atau 2^{96}, kunci pembungkus unik sebelum keausan kriptografi terjadi. Meskipun risiko kelelahan yang sangat rendah ini, Anda mungkin diminta untuk memutar kunci cabang aktif Anda karena aturan bisnis atau kontrak atau peraturan pemerintah.

Versi aktif dari kunci cabang tetap aktif sampai Anda memutarnya. Versi sebelumnya dari kunci cabang aktif tidak akan digunakan untuk melakukan operasi enkripsi dan tidak dapat digunakan untuk mendapatkan kunci pembungkus baru, tetapi mereka masih dapat ditanyakan dan menyediakan kunci pembungkus untuk mendekripsi kunci data yang mereka enkripsi saat aktif.

Izin yang diperlukan

Untuk memutar kunci cabang, Anda memerlukan ReEncrypt izin kms: GenerateDataKeyWithoutPlaintext dan kms: pada kunci KMS yang ditentukan dalam tindakan penyimpanan kunci Anda.

Putar tombol cabang aktif

Gunakan `VersionKey` operasi untuk memutar kunci cabang aktif Anda. Saat Anda memutar kunci cabang aktif, kunci cabang baru dibuat untuk menggantikan versi sebelumnya. `branch-key-id`Tidak berubah saat Anda memutar kunci cabang aktif. Anda harus menentukan `branch-key-id` yang mengidentifikasi kunci cabang aktif saat ini ketika Anda meneleponVersionKey.

Java

```
keystore.VersionKey(
    VersionKeyInput.builder()
        .branchKeyIdentifier("branch-key-id")
        .build()
);
```

C# / .NET

```
keystore.VersionKey(new VersionKeyInput{BranchKeyIdentifier = branchKeyId});
```

Python

```
keystore.version_key(
    VersionKeyInput(
        branch_key_identifier=branch_key_id
    )
)
```

Rust

```
keystore.version_key()
        .branch_key_identifier(branch_key_id)
        .send()
        .await?;
```

Go

```
_, err = keyStore.VersionKey(context.Background(), keystoretypes.VersionKeyInput{
    BranchKeyIdentifier: branchKeyId,
})
if err != nil {
    return err
}
```

Gantungan kunci

Implementasi bahasa pemrograman yang didukung menggunakan keyrings untuk melakukan enkripsi amplop. Keyrings menghasilkan, mengenkripsi, dan mendekripsi kunci data. Keyrings menentukan sumber kunci data unik yang melindungi setiap pesan, dan kunci pembungkus yang mengenkripsi kunci data tersebut. Anda menentukan keyring saat mengenkripsi dan keyring yang sama atau berbeda saat mendekripsi. Anda dapat menggunakan gantungan kunci yang disediakan SDK atau menulis gantungan kunci kustom Anda sendiri yang kompatibel.

Anda dapat menggunakan setiap keyring satu per satu atau menggabungkan keyrings menjadi multi-keyring. Meskipun sebagian besar keyrings dapat menghasilkan, mengenkripsi, dan mendekripsi kunci data, Anda dapat membuat keyring yang hanya melakukan satu operasi tertentu, seperti keyring yang hanya menghasilkan kunci data, dan menggunakan keyring tersebut dalam kombinasi dengan yang lain.

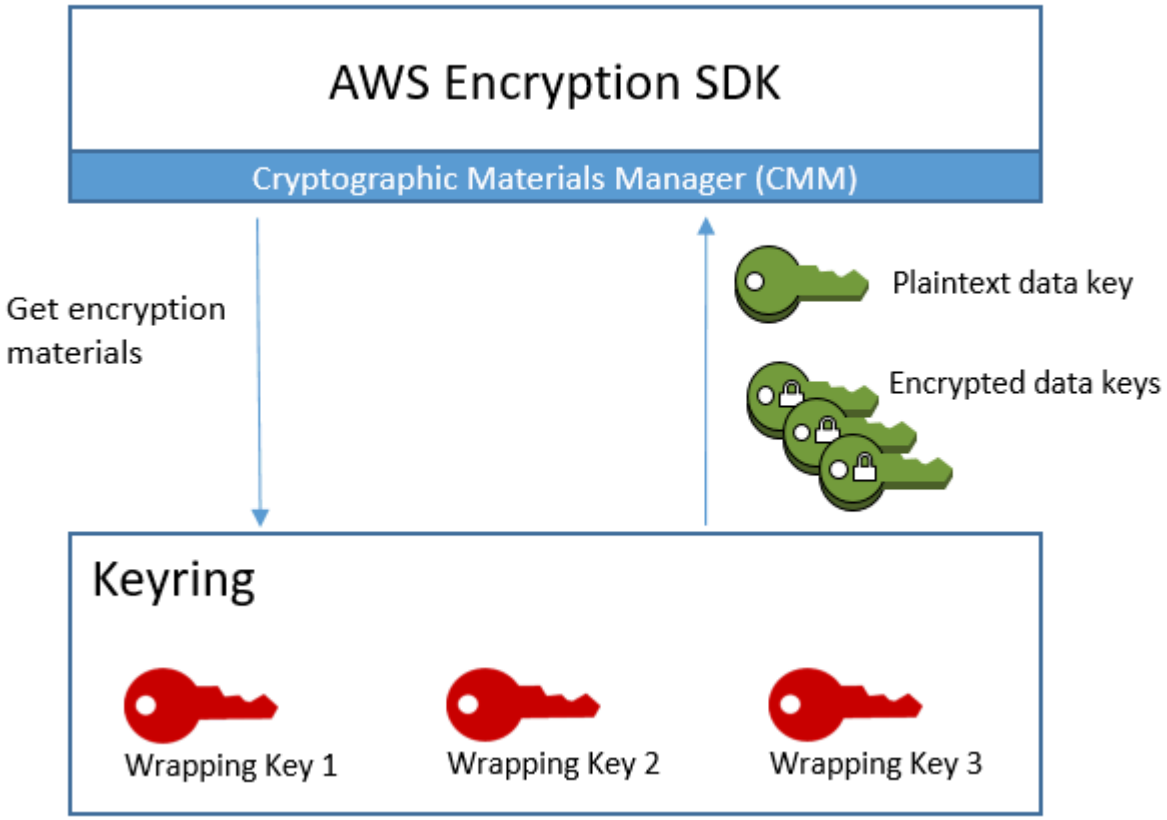
Kami menyarankan Anda menggunakan keyring yang melindungi kunci pembungkus Anda dan melakukan operasi kriptografi dalam batas aman, seperti AWS KMS keyring, yang menggunakan AWS KMS keys yang tidak pernah meninggalkan () tidak terenkripsi. AWS Key Management ServiceAWS KMS Anda juga dapat menulis keyring yang menggunakan kunci pembungkus yang disimpan dalam modul keamanan perangkat keras Anda (HSMs) atau dilindungi oleh layanan kunci utama lainnya. Untuk detailnya, lihat topik Antarmuka Keyring di AWS Encryption SDK Spesifikasi.

Keyrings memainkan peran kunci master dan penyedia kunci master yang digunakan dalam implementasi bahasa pemrograman lainnya. Jika Anda menggunakan implementasi bahasa yang berbeda AWS Encryption SDK untuk mengenkripsi dan mendekripsi data Anda, pastikan untuk menggunakan keyrings yang kompatibel dan penyedia kunci master. Lihat perinciannya di Kompatibilitas keyring.

Topik ini menjelaskan cara menggunakan fitur keyring AWS Encryption SDK dan cara memilih keyring.

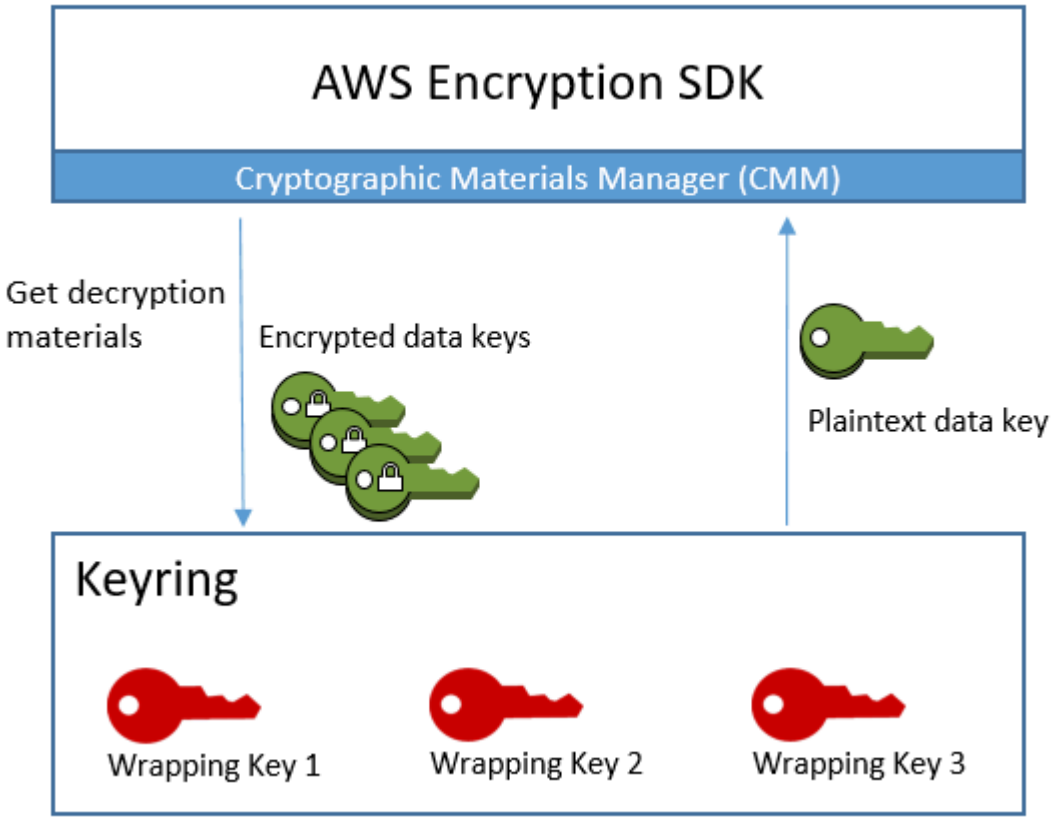
Cara kerja gantungan kunci

Ketika Anda mengenkripsi data, AWS Encryption SDK meminta keyring untuk materi enkripsi. Keyring mengembalikan kunci data plaintext dan salinan kunci data yang dienkripsi oleh masing-masing kunci pembungkus di keyring. AWS Encryption SDK Menggunakan kunci plaintext untuk mengenkripsi data, dan kemudian menghancurkan kunci data plaintext. Kemudian, AWS Encryption SDK mengembalikan pesan terenkripsi yang mencakup kunci data terenkripsi dan data terenkripsi.



Saat mendekripsi data, Anda dapat menggunakan keyring yang sama dengan yang Anda gunakan untuk mengenkripsi data, atau yang lain. Untuk mendekripsi data, keyring dekripsi harus menyertakan (atau memiliki akses ke) setidaknya satu kunci pembungkus dalam keyring enkripsi.

AWS Encryption SDK Lolos kunci data terenkripsi dari pesan terenkripsi ke keyring, dan meminta keyring untuk mendekripsi salah satu dari mereka. Keyring menggunakan kunci pembungkusnya untuk mendekripsi salah satu kunci data terenkripsi dan mengembalikan kunci data plaintext. AWS Encryption SDK Menggunakan kunci data plaintext untuk mendekripsi data. Jika tidak ada kunci pembungkus di keyring yang dapat mendekripsi salah satu kunci data terenkripsi, operasi dekripsi gagal.



Anda dapat menggunakan keyring tunggal atau juga menggabungkan keyrings dari jenis yang sama atau jenis yang berbeda ke dalam multi-keyring. Saat Anda mengenkripsi data, multi-keyring mengembalikan salinan kunci data yang dienkripsi oleh semua kunci pembungkus di semua keyring yang terdiri dari multi-keyring. Anda dapat mendekripsi data menggunakan keyring dengan salah satu tombol pembungkus di multi-keyring.

Kompatibilitas keyring

Meskipun implementasi bahasa yang berbeda AWS Encryption SDK memiliki beberapa perbedaan arsitektur, mereka sepenuhnya kompatibel, tunduk pada kendala bahasa. Anda dapat mengenkripsi data Anda menggunakan satu implementasi bahasa dan mendekripsi dengan implementasi bahasa lainnya. Namun, Anda harus menggunakan kunci pembungkus yang sama atau sesuai untuk mengenkripsi dan mendekripsi kunci data Anda. Untuk informasi tentang kendala bahasa, lihat topik tentang setiap implementasi bahasa, seperti the section called “Kompatibilitas” dalam topik. AWS Encryption SDK for JavaScript

Keyrings didukung dalam bahasa pemrograman berikut:

- AWS Encryption SDK for C
- AWS Encryption SDK for JavaScript
- AWS Encryption SDK untuk .NET
- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.
- AWS Encryption SDK untuk Rust
- AWS Encryption SDK untuk Go

Memvariasikan persyaratan untuk gantungan kunci enkripsi

Dalam implementasi AWS Encryption SDK bahasa selain AWS Encryption SDK for C, semua kunci pembungkus dalam keyring enkripsi (atau multi-keyring) atau penyedia kunci utama harus dapat mengenkripsi kunci data. Jika ada kunci pembungkus gagal untuk mengenkripsi, metode enkripsi gagal. Akibatnya, penelepon harus memiliki izin yang diperlukan untuk semua kunci di keyring. Jika Anda menggunakan keyring penemuan untuk mengenkripsi data, sendiri atau dalam multi-keyring, operasi enkripsi gagal.

Pengecualiannya adalah AWS Encryption SDK for C, di mana operasi enkripsi mengabaikan keyring penemuan standar, tetapi gagal jika Anda menentukan keyring penemuan Multi-wilayah, sendiri atau dalam multi-keyring.

Gantungan Kunci yang Kompatibel dan Penyedia Kunci Utama

Tabel berikut menunjukkan kunci master dan penyedia kunci master mana yang kompatibel dengan gantungan kunci yang disediakan AWS Encryption SDK . Setiap ketidakcocokan kecil karena kendala bahasa dijelaskan dalam topik tentang implementasi bahasa.

Gantungan kunci:	Penyedia Kunci Utama:
AWS KMS gantungan kunci	KMSMasterKunci (Java) KMSMasterKeyProvider (Jawa) KMSMasterKunci (Python) KMSMasterKeyProvider (Python)

Gantungan kunci:	Penyedia Kunci Utama:
	Note Itu AWS Encryption SDK for Python dan AWS Encryption SDK for Java tidak termasuk kunci master atau penyedia kunci master yang setara dengan keyring penemuan AWS KMS regional.
AWS KMS Gantungan kunci hierarkis	Didukung oleh bahasa dan versi pemrograman berikut: • Versi 3. x dari AWS Encryption SDK for Java • Versi 4. x dari AWS Encryption SDK untuk .NET • Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional. • Versi 1. x dari AWS Encryption SDK untuk Rust • Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go
AWS KMS Gantungan kunci ECDH	Didukung oleh bahasa dan versi pemrograman berikut: • Versi 3. x dari AWS Encryption SDK for Java • Versi 4. x dari AWS Encryption SDK untuk .NET • Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional. • Versi 1. x dari AWS Encryption SDK untuk Rust • Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go
Gantungan kunci AES mentah	Ketika mereka digunakan dengan kunci enkripsi simetris: JceMasterKey(Jawa) RawMasterKey(Python)

Gantungan kunci:	Penyedia Kunci Utama:
Gantungan kunci RSA mentah	Ketika mereka digunakan dengan kunci enkripsi asimetris: JceMasterKey(Jawa) RawMasterKey(Python) **Note** Raw RSA keyring tidak mendukung kunci KMS asimetris. Jika Anda ingin menggunakan tombol KMS RSA asimetris, versi 4. x dari AWS Encryption SDK untuk .NET mendukung AWS KMS keyrings yang menggunakan enkripsi simetris (`SYMMETRIC_DEFAULT`) atau RSA asimetris. AWS KMS keys
Gantungan kunci ECDH mentah	Didukung oleh bahasa dan versi pemrograman berikut: • Versi 3. x dari AWS Encryption SDK for Java • Versi 4. x dari AWS Encryption SDK untuk .NET • Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional. • Versi 1. x dari AWS Encryption SDK untuk Rust • Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

AWS KMS gantungan kunci

AWS KMS Keyring digunakan AWS KMS keysuntuk menghasilkan, mengenkripsi, dan mendekripsi kunci data. AWS Key Management Service (AWS KMS) melindungi kunci KMS Anda dan melakukan operasi kriptografi dalam batas FIPS. Kami menyarankan Anda menggunakan AWS KMS keyring, atau keyring dengan properti keamanan serupa, bila memungkinkan.

Semua implementasi bahasa pemrograman yang mendukung keyrings, mendukung AWS KMS keyrings yang menggunakan kunci KMS enkripsi simetris. Implementasi bahasa pemrograman berikut juga mendukung AWS KMS keyrings yang menggunakan kunci KMS RSA asimetris:

- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK untuk .NET
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.
- Versi 1. x dari AWS Encryption SDK untuk Rust
- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Jika Anda mencoba memasukkan kunci KMS asimetris dalam keyring enkripsi dalam implementasi bahasa lain, panggilan enkripsi gagal. Jika Anda memasukkannya ke dalam keyring dekripsi, itu diabaikan.

Anda dapat menggunakan kunci AWS KMS Multi-region di AWS KMS keyring atau penyedia kunci master yang dimulai pada versi 2.3. x dari AWS Encryption SDK dan versi 3.0. x dari CLI AWS Enkripsi. Untuk detail dan contoh penggunaan multi-Region-aware simbol, lihatMenggunakan Multi-region AWS KMS keys. Untuk informasi tentang kunci Multi-region, lihat Menggunakan kunci Multi-region di Panduan AWS Key Management Service Pengembang.

> **Note**
>
> Semua penyebutan gantungan kunci KMS dalam AWS Encryption SDK referensi ke keyrings. AWS KMS

AWS KMS gantungan kunci dapat mencakup dua jenis kunci pembungkus:

- Kunci generator: Menghasilkan kunci data teks biasa dan mengenkripsinya. Sebuah keyring yang mengenkripsi data harus memiliki satu kunci generator.
- Kunci tambahan: Mengenkripsi kunci data teks biasa yang dihasilkan oleh kunci generator. AWS KMS keyrings dapat memiliki nol atau lebih tombol tambahan.

Anda menggunakan harus memiliki kunci generator untuk mengenkripsi pesan. Ketika AWS KMS keyring hanya memiliki satu kunci KMS, kunci itu digunakan untuk menghasilkan dan mengenkripsi kunci data. Saat mendekripsi, kunci generator adalah opsional, dan perbedaan antara kunci generator dan kunci tambahan diabaikan.

Seperti semua gantungan kunci, AWS KMS gantungan kunci dapat digunakan secara independen atau dalam multi-keyring dengan gantungan kunci lain dari jenis yang sama atau berbeda.

Topik

Izin yang diperlukan untuk keyrings AWS KMS

AWS Encryption SDK Itu tidak memerlukan Akun AWS dan itu tidak tergantung pada apa pun Layanan AWS. Namun, untuk menggunakan AWS KMS keyring, Anda memerlukan izin minimum Akun AWS dan berikut pada keyring Anda. AWS KMS keys

- Untuk mengenkripsi dengan AWS KMS keyring, Anda memerlukan GenerateDataKey izin kms: pada kunci generator. Anda memerlukan izin KMS: Encrypt pada semua kunci tambahan di keyring. AWS KMS
- Untuk mendekripsi dengan AWS KMS keyring, Anda memerlukan izin KMS: Decrypt pada setidaknya satu kunci di keyring. AWS KMS
- Untuk mengenkripsi dengan multi-keyring yang terdiri dari AWS KMS keyrings, Anda memerlukan GenerateDataKey izin kms: pada kunci generator di keyring generator. Anda memerlukan izin KMS: Encrypt pada semua kunci lain di semua keyrings lainnya. AWS KMS
- Untuk mengenkripsi dengan AWS KMS keyring RSA asimetris, Anda tidak perlu kms: GenerateDataKey atau KMS:Encrypt karena Anda harus menentukan materi kunci publik yang ingin Anda gunakan untuk enkripsi saat Anda membuat keyring. Tidak ada AWS KMS panggilan yang dilakukan saat mengenkripsi dengan keyring ini. Untuk mendekripsi dengan AWS KMS keyring RSA asimetris, Anda memerlukan izin KMS: Dekripsi.

Untuk informasi selengkapnya tentang izin AWS KMS keys, lihat akses kunci KMS dan izin di Panduan Pengembang.AWS Key Management Service

Mengidentifikasi AWS KMS keys dalam AWS KMS keyring

AWS KMS Keyring dapat mencakup satu atau lebih AWS KMS keys. Untuk menentukan AWS KMS key dalam AWS KMS keyring, gunakan pengenal AWS KMS kunci yang didukung. Pengidentifikasi kunci yang dapat Anda gunakan untuk mengidentifikasi AWS KMS key dalam keyring bervariasi

dengan operasi dan implementasi bahasa. Untuk detail tentang pengidentifikasi kunci AWS KMS key, lihat Pengidentifikasi Kunci di Panduan AWS Key Management Service Pengembang.

Sebagai praktik terbaik, gunakan pengenal kunci paling spesifik yang praktis untuk tugas Anda.

- Dalam keyring enkripsi untuk AWS Encryption SDK for C, Anda dapat menggunakan kunci ARN atau alias ARN untuk mengidentifikasi kunci KMS. Dalam semua implementasi bahasa lainnya, Anda dapat menggunakan ID kunci, ARN kunci, nama alias, atau alias ARN untuk mengenkripsi data.
- Dalam keyring dekripsi, Anda harus menggunakan ARN kunci untuk mengidentifikasi. AWS KMS keys Persyaratan ini berlaku untuk semua implementasi bahasa dari. AWS Encryption SDK Lihat perinciannya di Memilih tombol pembungkus.
- Dalam keyring yang digunakan untuk enkripsi dan dekripsi, Anda harus menggunakan ARN kunci untuk mengidentifikasi. AWS KMS keys Persyaratan ini berlaku untuk semua implementasi bahasa dari. AWS Encryption SDK

Jika Anda menentukan nama alias atau alias ARN untuk kunci KMS dalam keyring enkripsi, operasi enkripsi menyimpan ARN kunci yang saat ini terkait dengan alias dalam metadata kunci data terenkripsi. Itu tidak menyimpan alias. Perubahan pada alias tidak memengaruhi kunci KMS yang digunakan untuk mendekripsi kunci data terenkripsi Anda.

Membuat AWS KMS keyring

Anda dapat mengonfigurasi setiap AWS KMS keyring dengan satu AWS KMS key atau beberapa AWS KMS keys yang sama atau berbeda Akun AWS dan Wilayah AWS. AWS KMS keys Harus berupa kunci KMS enkripsi simetris (SYMMETRIC_DEFAULT) atau kunci KMS RSA asimetris. Anda juga dapat menggunakan enkripsi simetris Multi-region KMS key. Anda dapat menggunakan satu atau lebih AWS KMS keyring dalam multi-keyring.

Anda dapat membuat AWS KMS keyring yang mengenkripsi dan mendekripsi data, atau Anda dapat membuat AWS KMS gantungan kunci khusus untuk mengenkripsi atau mendekripsi. Saat Anda membuat AWS KMS keyring untuk mengenkripsi data, Anda harus menentukan kunci generator, AWS KMS key yang digunakan untuk menghasilkan kunci data plaintext dan mengenkripsinya. Kunci data secara matematis tidak terkait dengan kunci KMS. Kemudian, jika Anda memilih, Anda dapat menentukan tambahan AWS KMS keys yang mengenkripsi kunci data teks biasa yang sama. Untuk mendekripsi bidang terenkripsi yang dilindungi oleh keyring ini, keyring dekripsi yang Anda gunakan harus menyertakan setidaknya satu dari yang ditentukan dalam keyring, atau tidak. AWS KMS keys

AWS KMS keys(AWS KMS Gantungan kunci tanpa AWS KMS keys dikenal sebagai gantungan kunci AWS KMS penemuan.)

Dalam implementasi AWS Encryption SDK bahasa selain AWS Encryption SDK for C, semua kunci pembungkus dalam keyring enkripsi atau multi-keyring harus dapat mengenkripsi kunci data. Jika ada kunci pembungkus gagal untuk mengenkripsi, metode enkripsi gagal. Akibatnya, penelepon harus memiliki izin yang diperlukan untuk semua kunci di keyring. Jika Anda menggunakan keyring penemuan untuk mengenkripsi data, sendiri atau dalam multi-keyring, operasi enkripsi gagal. Pengecualiannya adalah AWS Encryption SDK for C, di mana operasi enkripsi mengabaikan keyring penemuan standar, tetapi gagal jika Anda menentukan keyring penemuan Multi-wilayah, sendiri atau dalam multi-keyring.

Contoh berikut membuat AWS KMS keyring dengan kunci generator dan satu kunci tambahan. Baik kunci generator dan kunci tambahan adalah kunci KMS enkripsi simetris. Contoh-contoh ini menggunakan kunci ARNs untuk mengidentifikasi kunci KMS. Ini adalah praktik terbaik untuk AWS KMS gantungan kunci yang digunakan untuk enkripsi, dan persyaratan untuk AWS KMS gantungan kunci yang digunakan untuk dekripsi. Lihat perinciannya di Mengidentifikasi AWS KMS keys dalam AWS KMS keyring.

C

Untuk mengidentifikasi AWS KMS key dalam keyring enkripsi di AWS Encryption SDK for C, tentukan kunci ARN atau alias ARN. Dalam keyring dekripsi, Anda harus menggunakan kunci ARN. Lihat perinciannya di Mengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Untuk contoh lengkap, lihat string.cpp.

```
const char * generator_key = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"

const char * additional_key = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"

struct aws_cryptosdk_keyring *kms_encrypt_keyring =
       Aws::Cryptosdk::KmsKeyring::Builder().Build(generator_key,{additional_key});
```

C# / .NET

Untuk membuat keyring dengan satu atau lebih kunci KMS di AWS Encryption SDK for .NET, gunakan metode ini`CreateAwsKmsMultiKeyring()`. Contoh ini menggunakan dua AWS

KMS kunci. Untuk menentukan satu kunci KMS, gunakan hanya `Generator` parameter. `KmsKeyIds`Parameter yang menentukan kunci KMS tambahan adalah opsional.

Input untuk keyring ini tidak membutuhkan AWS KMS klien. Sebaliknya, AWS Encryption SDK menggunakan AWS KMS klien default untuk setiap Wilayah diwakili oleh kunci KMS di keyring. Misalnya, jika kunci KMS yang diidentifikasi oleh nilai `Generator` parameter berada di Wilayah AS Barat (Oregon) (`us-west-2`), akan AWS Encryption SDK membuat AWS KMS klien default untuk Wilayah tersebut`us-west-2`. Jika Anda perlu menyesuaikan AWS KMS klien, gunakan `CreateAwsKmsKeyring()` metode ini.

Saat Anda menentukan AWS KMS key untuk keyring enkripsi di AWS Encryption SDK for .NET, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci, nama alias, atau alias ARN. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Contoh berikut menggunakan versi 4. x AWS Encryption SDK untuk .NET dan `CreateAwsKmsKeyring()` metode untuk menyesuaikan AWS KMS klien.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

string generatorKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
List<string> additionalKeys = new List<string> { "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321" };

// Instantiate the keyring input object
var createEncryptKeyringInput = new CreateAwsKmsMultiKeyringInput
{
    Generator = generatorKey,
    KmsKeyIds = additionalKeys
};

var kmsEncryptKeyring = mpl.CreateAwsKmsMultiKeyring(createEncryptKeyringInput);
```

JavaScript Browser

Saat Anda menentukan AWS KMS key untuk gantungan kunci enkripsi di AWS Encryption SDK for JavaScript, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci,

nama alias, atau alias ARN. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

Untuk contoh lengkap, lihat kms_simple.ts di repositori di. AWS Encryption SDK for JavaScript GitHub

```
import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const clientProvider = getClient(KMS, { credentials })
const generatorKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
const additionalKey = 'alias/exampleAlias'

const keyring = new KmsKeyringBrowser({
  clientProvider,
  generatorKeyId,
  keyIds: [additionalKey]
})
```

JavaScript Node.js

Saat Anda menentukan AWS KMS key untuk gantungan kunci enkripsi di AWS Encryption SDK for JavaScript, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci, nama alias, atau alias ARN. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient`

untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

Untuk contoh lengkap, lihat kms_simple.ts di repositori di. AWS Encryption SDK for JavaScript GitHub

```
import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const generatorKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

const additionalKey = 'alias/exampleAlias'

const keyring = new KmsKeyringNode({
  generatorKeyId,
  keyIds: [additionalKey]
})
```

Java

Untuk membuat keyring dengan satu atau lebih AWS KMS tombol, gunakan `CreateAwsKmsMultiKeyring()` metode ini. Contoh ini menggunakan dua kunci KMS. Untuk menentukan satu kunci KMS, gunakan hanya `generator` parameter. `kmsKeyIds`Parameter yang menentukan kunci KMS tambahan adalah opsional.

Input untuk keyring ini tidak membutuhkan AWS KMS klien. Sebaliknya, AWS Encryption SDK menggunakan AWS KMS klien default untuk setiap Wilayah diwakili oleh kunci KMS di keyring. Misalnya, jika kunci KMS yang diidentifikasi oleh nilai `Generator` parameter berada di Wilayah AS Barat (Oregon) (`us-west-2`), akan AWS Encryption SDK membuat AWS KMS klien default untuk Wilayah tersebut`us-west-2`. Jika Anda perlu menyesuaikan AWS KMS klien, gunakan `CreateAwsKmsKeyring()` metode ini.

Saat Anda menentukan AWS KMS key untuk gantungan kunci enkripsi di AWS Encryption SDK for Java, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci, nama alias,

atau alias ARN. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Untuk contoh lengkap, lihat BasicEncryptionKeyringExample.java di AWS Encryption SDK for Java repositori di. GitHub

```
// Instantiate the AWS Encryption SDK and material providers
final AwsCrypto crypto = AwsCrypto.builder().build();
final MaterialProviders materialProviders = MaterialProviders.builder()
            .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
            .build();

String generatorKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
List<String> additionalKey = Collections.singletonList("arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321");
// Create the keyring
final CreateAwsKmsMultiKeyringInput keyringInput =
 CreateAwsKmsMultiKeyringInput.builder()
        .generator(generatorKey)
        .kmsKeyIds(additionalKey)
        .build();
final IKeyring kmsKeyring =
 materialProviders.CreateAwsKmsMultiKeyring(keyringInput);
```

Python

Untuk membuat keyring dengan satu atau lebih AWS KMS tombol, gunakan `create_aws_kms_multi_keyring()` metode ini. Contoh ini menggunakan dua kunci KMS. Untuk menentukan satu kunci KMS, gunakan hanya `generator` parameter. `kms_key_ids`Parameter yang menentukan kunci KMS tambahan adalah opsional.

Input untuk keyring ini tidak membutuhkan AWS KMS klien. Sebaliknya, AWS Encryption SDK menggunakan AWS KMS klien default untuk setiap Wilayah diwakili oleh kunci KMS di keyring. Misalnya, jika kunci KMS yang diidentifikasi oleh nilai `generator` parameter berada di Wilayah AS Barat (Oregon) (`us-west-2`), akan AWS Encryption SDK membuat AWS KMS klien default untuk Wilayah tersebut`us-west-2`. Jika Anda perlu menyesuaikan AWS KMS klien, gunakan `create_aws_kms_keyring()` metode ini.

Saat Anda menentukan AWS KMS key untuk gantungan kunci enkripsi di AWS Encryption SDK for Python, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci,

nama alias, atau alias ARN. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Contoh berikut membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. `REQUIRE_ENCRYPT_REQUIRE_DECRYPT` Untuk contoh lengkap, lihat aws_kms_multi_keyring_example.py di AWS Encryption SDK for Python repositori di. GitHub

```
# Instantiate the AWS Encryption SDK client
client = aws_encryption_sdk.EncryptionSDKClient(
    commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

# Optional: Create an encryption context
encryption_context: Dict[str, str] = {
    "encryption": "context",
    "is not": "secret",
    "but adds": "useful metadata",
    "that can help you": "be confident that",
    "the data you are handling": "is what you think it is",
}

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create the AWS KMS keyring
kms_multi_keyring_input: CreateAwsKmsMultiKeyringInput =
 CreateAwsKmsMultiKeyringInput(
    generator="arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    kms_key_ids="arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
)

kms_multi_keyring: IKeyring = mat_prov.create_aws_kms_multi_keyring(
    input=kms_multi_keyring_input
)
```

Rust

Untuk membuat keyring dengan satu atau lebih AWS KMS tombol, gunakan `create_aws_kms_multi_keyring()` metode ini. Contoh ini menggunakan dua kunci

KMS. Untuk menentukan satu kunci KMS, gunakan hanya `generator` parameter. `kms_key_ids`Parameter yang menentukan kunci KMS tambahan adalah opsional.

Input untuk keyring ini tidak membutuhkan AWS KMS klien. Sebaliknya, AWS Encryption SDK menggunakan AWS KMS klien default untuk setiap Wilayah diwakili oleh kunci KMS di keyring. Misalnya, jika kunci KMS yang diidentifikasi oleh nilai `generator` parameter berada di Wilayah AS Barat (Oregon) (`us-west-2`), akan AWS Encryption SDK membuat AWS KMS klien default untuk Wilayah tersebut`us-west-2`. Jika Anda perlu menyesuaikan AWS KMS klien, gunakan `create_aws_kms_keyring()` metode ini.

Saat Anda menentukan keyring enkripsi AWS KMS key untuk Rust, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci, nama alias, atau alias ARN. AWS Encryption SDK Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Contoh berikut membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. `REQUIRE_ENCRYPT_REQUIRE_DECRYPT` Untuk contoh lengkapnya, lihat aws_kms_keyring_example.rs di direktori Rust dari repositori di. aws-encryption-sdk GitHub

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create an AWS KMS client
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Optional: Create an encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;
```

```
// Create the AWS KMS keyring
let kms_keyring = mpl
    .create_aws_kms_keyring()
    .kms_key_id(kms_key_id)
    .kms_client(kms_client)
    .send()
    .await?;

kms_multi_keyring: IKeyring = mpl.create_aws_kms_multi_keyring(
    input=kms_multi_keyring_input
)
```

Go

Untuk membuat keyring dengan satu atau lebih AWS KMS tombol, gunakan `create_aws_kms_multi_keyring()` metode ini. Contoh ini menggunakan dua kunci KMS. Untuk menentukan satu kunci KMS, gunakan hanya `generator` parameter. `kms_key_ids`Parameter yang menentukan kunci KMS tambahan adalah opsional.

Input untuk keyring ini tidak membutuhkan AWS KMS klien. Sebaliknya, AWS Encryption SDK menggunakan AWS KMS klien default untuk setiap Wilayah diwakili oleh kunci KMS di keyring. Misalnya, jika kunci KMS yang diidentifikasi oleh nilai `generator` parameter berada di Wilayah AS Barat (Oregon) (`us-west-2`), akan AWS Encryption SDK membuat AWS KMS klien default untuk Wilayah tersebut`us-west-2`. Jika Anda perlu menyesuaikan AWS KMS klien, gunakan `create_aws_kms_keyring()` metode ini.

Saat Anda menentukan keyring enkripsi AWS KMS keyAWS Encryption SDK untuk Go, Anda dapat menggunakan pengenal kunci yang valid: ID kunci, ARN kunci, nama alias, atau aliasARN. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Contoh berikut membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. `REQUIRE_ENCRYPT_REQUIRE_DECRYPT`

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
```

```
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create the AWS KMS keyring
awsKmsMultiKeyringInput := mpltypes.CreateAwsKmsMultiKeyringInput{
    Generator: "&arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    KmsKeyIds: []string{"arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"},
}
awsKmsMultiKeyring, err := matProv.CreateAwsKmsMultiKeyring(context.Background(),
 awsKmsMultiKeyringInput)
```

Ini AWS Encryption SDK juga mendukung AWS KMS keyrings yang menggunakan tombol RSA KMS asimetris. AWS KMS Keyring RSA asimetris hanya dapat berisi satu key pair.

Untuk mengenkripsi dengan AWS KMS keyring RSA asimetris, Anda tidak perlu kms: GenerateDataKey atau KMS:Encrypt karena Anda harus menentukan materi kunci publik yang ingin Anda gunakan untuk enkripsi saat Anda membuat keyring. Tidak ada AWS KMS panggilan yang dilakukan saat mengenkripsi dengan keyring ini. Untuk mendekripsi dengan AWS KMS keyring RSA asimetris, Anda memerlukan izin KMS: Dekripsi.

> **Note**
>
> Untuk membuat AWS KMS keyring yang menggunakan kunci KMS RSA asimetris, Anda harus menggunakan salah satu implementasi bahasa pemrograman berikut:
>
> - Versi 3. x dari AWS Encryption SDK for Java
> - Versi 4. x dari AWS Encryption SDK untuk .NET
> - Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.
> - Versi 1. x dari AWS Encryption SDK untuk Rust
> - Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Contoh berikut menggunakan `CreateAwsKmsRsaKeyring` metode untuk membuat AWS KMS keyring dengan kunci KMS RSA asimetris. Untuk membuat AWS KMS keyring RSA asimetris, berikan nilai berikut.

- `kmsClient`: buat AWS KMS klien baru
- `kmsKeyID`: kunci ARN yang mengidentifikasi kunci KMS RSA asimetris Anda
- `publicKey`: file PEM yang dikodekan UTF-8 yang mewakili kunci publik dari kunci yang Anda berikan ByteBuffer `kmsKeyID`
- `encryptionAlgorithm`: algoritma enkripsi harus `RSAES_OAEP_SHA_256` atau `RSAES_OAEP_SHA_1`

C# / .NET

Untuk membuat AWS KMS keyring RSA asimetris, Anda harus memberikan kunci publik dan kunci pribadi ARN dari kunci KMS RSA asimetris Anda. Kunci publik harus dikodekan PEM. Contoh berikut membuat AWS KMS keyring dengan asimetris RSA key pair.

```
// Instantiate the AWS Encryption SDK and material providers
```

```
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

var publicKey = new MemoryStream(Encoding.UTF8.GetBytes(AWS KMS RSA public key));

// Instantiate the keyring input object
var createKeyringInput = new CreateAwsKmsRsaKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = AWS KMS RSA private key ARN,
    PublicKey = publicKey,
    EncryptionAlgorithm = EncryptionAlgorithmSpec.RSAES_OAEP_SHA_256
};

// Create the keyring
var kmsRsaKeyring = mpl.CreateAwsKmsRsaKeyring(createKeyringInput);
```

Java

Untuk membuat AWS KMS keyring RSA asimetris, Anda harus memberikan kunci publik dan kunci pribadi ARN dari kunci KMS RSA asimetris Anda. Kunci publik harus dikodekan PEM. Contoh berikut membuat AWS KMS keyring dengan asimetris RSA key pair.

```
// Instantiate the AWS Encryption SDK and material providers
final AwsCrypto crypto = AwsCrypto.builder()
        // Specify algorithmSuite without asymmetric signing here
        //
        // ALG_AES_128_GCM_IV12_TAG16_NO_KDF("0x0014"),
        // ALG_AES_192_GCM_IV12_TAG16_NO_KDF("0x0046"),
        // ALG_AES_256_GCM_IV12_TAG16_NO_KDF("0x0078"),
        // ALG_AES_128_GCM_IV12_TAG16_HKDF_SHA256("0x0114"),
        // ALG_AES_192_GCM_IV12_TAG16_HKDF_SHA256("0x0146"),
        // ALG_AES_256_GCM_IV12_TAG16_HKDF_SHA256("0x0178")

 .withEncryptionAlgorithm(CryptoAlgorithm.ALG_AES_256_GCM_IV12_TAG16_HKDF_SHA256)
        .build();

final MaterialProviders matProv = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();

// Create a KMS RSA keyring.
//    This keyring takes in:
```

```
//     - kmsClient
//     - kmsKeyId: Must be an ARN representing an asymmetric RSA KMS key
//     - publicKey: A ByteBuffer of a UTF-8 encoded PEM file representing the public
//                  key for the key passed into kmsKeyId
//     - encryptionAlgorithm: Must be either RSAES_OAEP_SHA_256 or RSAES_OAEP_SHA_1
final CreateAwsKmsRsaKeyringInput createAwsKmsRsaKeyringInput =
        CreateAwsKmsRsaKeyringInput.builder()
                .kmsClient(KmsClient.create())
                .kmsKeyId(rsaKeyArn)
                .publicKey(publicKey)
                .encryptionAlgorithm(EncryptionAlgorithmSpec.RSAES_OAEP_SHA_256)
                .build();
IKeyring awsKmsRsaKeyring =
 matProv.CreateAwsKmsRsaKeyring(createAwsKmsRsaKeyringInput);
```

Python

Untuk membuat AWS KMS keyring RSA asimetris, Anda harus memberikan kunci publik dan kunci pribadi ARN dari kunci KMS RSA asimetris Anda. Kunci publik harus dikodekan PEM. Contoh berikut membuat AWS KMS keyring dengan asimetris RSA key pair.

```
# Instantiate the AWS Encryption SDK client
client = aws_encryption_sdk.EncryptionSDKClient(
    commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

# Optional: Create an encryption context
encryption_context: Dict[str, str] = {
    "encryption": "context",
    "is not": "secret",
    "but adds": "useful metadata",
    "that can help you": "be confident that",
    "the data you are handling": "is what you think it is",
}

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create the AWS KMS keyring
keyring_input: CreateAwsKmsRsaKeyringInput = CreateAwsKmsRsaKeyringInput(
    public_key="public_key",
```

```
    kms_key_id="kms_key_id",
    encryption_algorithm="RSAES_OAEP_SHA_256",
    kms_client=kms_client
)

kms_rsa_keyring: IKeyring = mat_prov.create_aws_kms_rsa_keyring(
    input=keyring_input
)
```

Rust

Untuk membuat AWS KMS keyring RSA asimetris, Anda harus memberikan kunci publik dan kunci pribadi ARN dari kunci KMS RSA asimetris Anda. Kunci publik harus dikodekan PEM. Contoh berikut membuat AWS KMS keyring dengan asimetris RSA key pair.

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create an AWS KMS client
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Optional: Create an encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create the AWS KMS keyring
let kms_rsa_keyring = mpl
    .create_aws_kms_rsa_keyring()
    .kms_key_id(kms_key_id)
    .public_key(aws_smithy_types::Blob::new(public_key))
```

```
 .encryption_algorithm(aws_sdk_kms::types::EncryptionAlgorithmSpec::RsaesOaepSha256)
    .kms_client(kms_client)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
```

```
    "that can help you":         "be confident that",
    "the data you are handling": "is what you think it is",
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create the AWS KMS keyring
awsKmsRSAKeyringInput := mpltypes.CreateAwsKmsRsaKeyringInput{
    KmsClient:           kmsClient,
    KmsKeyId:            kmsKeyID,
    PublicKey:           kmsPublicKey,
    EncryptionAlgorithm: kmstypes.EncryptionAlgorithmSpecRsaesOaepSha256,
}
awsKmsRSAKeyring, err := matProv.CreateAwsKmsRsaKeyring(context.Background(),
 awsKmsRSAKeyringInput)
if err != nil {
    panic(err)
}
```

Menggunakan AWS KMS keyring penemuan

Saat mendekripsi, ini adalah praktik terbaik untuk menentukan kunci pembungkus yang dapat digunakan. AWS Encryption SDK Untuk mengikuti praktik terbaik ini, gunakan keyring AWS KMS dekripsi yang membatasi kunci AWS KMS pembungkus ke kunci yang Anda tentukan. Namun, Anda juga dapat membuat keyring AWS KMS penemuan, yaitu AWS KMS keyring yang tidak menentukan kunci pembungkus apa pun.

AWS Encryption SDK Ini menyediakan keyring AWS KMS penemuan standar dan keyring penemuan untuk kunci AWS KMS Multi-wilayah. Untuk informasi tentang menggunakan kunci Multi-wilayah dengan AWS Encryption SDK, lihatMenggunakan Multi-region AWS KMS keys.

Karena tidak menentukan kunci pembungkus apa pun, keyring penemuan tidak dapat mengenkripsi data. Jika Anda menggunakan keyring penemuan untuk mengenkripsi data, sendiri atau dalam multi-keyring, operasi enkripsi gagal. Pengecualiannya adalah AWS Encryption SDK for C, di mana operasi enkripsi mengabaikan keyring penemuan standar, tetapi gagal jika Anda menentukan keyring penemuan Multi-wilayah, sendiri atau dalam multi-keyring.

Saat mendekripsi, keyring penemuan memungkinkan AWS Encryption SDK untuk meminta AWS KMS untuk mendekripsi kunci data terenkripsi apa pun dengan menggunakan yang mengenkripsi itu, terlepas dari siapa AWS KMS key yang memiliki atau memiliki akses ke sana. AWS KMS key Panggilan hanya berhasil ketika penelepon memiliki `kms:Decrypt` izin pada. AWS KMS key

> **Important**
>
> Jika Anda menyertakan keyring AWS KMS penemuan dalam multi-keyring dekripsi, keyring penemuan mengesampingkan semua batasan kunci KMS yang ditentukan oleh gantungan kunci lain di multi-keyring. Multi-keyring berperilaku seperti keyring yang paling tidak membatasi. Keyring AWS KMS penemuan tidak berpengaruh pada enkripsi saat digunakan sendiri atau dalam multi-keyring.

AWS Encryption SDK Ini menyediakan keyring AWS KMS penemuan untuk kenyamanan. Namun, kami menyarankan Anda menggunakan keyring yang lebih terbatas bila memungkinkan karena alasan berikut.

- Keaslian — Keyring AWS KMS penemuan dapat menggunakan apa pun AWS KMS key yang digunakan untuk mengenkripsi kunci data dalam pesan terenkripsi, sehingga penelepon memiliki izin untuk menggunakannya untuk mendekripsi. AWS KMS key Ini mungkin bukan AWS KMS key yang ingin digunakan oleh penelepon. Misalnya, salah satu kunci data terenkripsi mungkin telah dienkripsi di bawah yang kurang aman AWS KMS key yang dapat digunakan siapa pun.
- Latensi dan kinerja — Keyring AWS KMS penemuan mungkin terlihat lebih lambat daripada keyring lain karena AWS Encryption SDK mencoba mendekripsi semua kunci data terenkripsi, termasuk yang dienkripsi oleh AWS KMS keys di lain Akun AWS dan Wilayah, dan AWS KMS keys penelepon tidak memiliki izin untuk digunakan untuk dekripsi.

Jika Anda menggunakan keyring penemuan, kami sarankan Anda menggunakan filter penemuan untuk membatasi kunci KMS yang dapat digunakan untuk kunci yang ditentukan Akun AWS dan partisi. Filter penemuan didukung dalam versi 1.7. x dan kemudian AWS Encryption SDK. Untuk bantuan menemukan ID akun dan partisi Anda, lihat Akun AWS Pengenal Anda dan format ARN di. Referensi Umum AWS

Kode berikut membuat instance keyring penemuan dengan filter AWS KMS penemuan yang membatasi kunci KMS yang AWS Encryption SDK dapat digunakan untuk yang ada di `aws` partisi dan akun contoh 111122223333.

Sebelum menggunakan kode ini, ganti contoh Akun AWS dan nilai partisi dengan nilai yang valid untuk Anda Akun AWS dan partisi. Jika kunci KMS Anda berada di Wilayah Tiongkok, gunakan nilai `aws-cn` partisi. Jika kunci KMS Anda masuk AWS GovCloud (US) Regions, gunakan nilai `aws-us-gov` partisi. Untuk yang lainnya Wilayah AWS, gunakan nilai `aws` partisi.

C

Untuk contoh lengkap, lihat: kms_discovery.cpp.

```
std::shared_ptr<KmsKeyring::> discovery_filter(
    KmsKeyring::DiscoveryFilter::Builder("aws")
        .AddAccount("111122223333")
        .Build());

struct aws_cryptosdk_keyring *kms_discovery_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder()
       .BuildDiscovery(discovery_filter));
```

C# / .NET

Contoh berikut menggunakan versi 4. x dari AWS Encryption SDK untuk .NET.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

List<string> account = new List<string> { "111122223333" };

// In a discovery keyring, you specify an AWS KMS client and a discovery filter,
// but not a AWS KMS key
var kmsDiscoveryKeyringInput = new CreateAwsKmsDiscoveryKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    DiscoveryFilter = new DiscoveryFilter()
    {
        AccountIds = account,
        Partition = "aws"
    }
};

var kmsDiscoveryKeyring =
 mpl.CreateAwsKmsDiscoveryKeyring(kmsDiscoveryKeyringInput);
```

JavaScript Browser

Dalam JavaScript, Anda harus secara eksplisit menentukan properti penemuan.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

```
import {
  KmsKeyringBrowser,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-browser'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const clientProvider = getClient(KMS, { credentials })

const discovery = true
const keyring = new KmsKeyringBrowser(clientProvider, {
    discovery,
    discoveryFilter: { accountIDs: [111122223333], partition: 'aws' }
})
```

JavaScript Node.js

Dalam JavaScript, Anda harus secara eksplisit menentukan properti penemuan.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

```
import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
```

```
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const discovery = true

const keyring = new KmsKeyringNode({
    discovery,
    discoveryFilter: { accountIDs: ['111122223333'], partition: 'aws' }
})
```

Java

```
// Create discovery filter
DiscoveryFilter discoveryFilter = DiscoveryFilter.builder()
        .partition("aws")
        .accountIds(111122223333)
        .build();
// Create the discovery keyring
CreateAwsKmsMrkDiscoveryMultiKeyringInput createAwsKmsMrkDiscoveryMultiKeyringInput
 = CreateAwsKmsMrkDiscoveryMultiKeyringInput.builder()
        .discoveryFilter(discoveryFilter)
        .build();
IKeyring decryptKeyring =
 matProv.CreateAwsKmsMrkDiscoveryMultiKeyring(createAwsKmsMrkDiscoveryMultiKeyringInput);
```

Python

```
# Instantiate the AWS Encryption SDK
client = aws_encryption_sdk.EncryptionSDKClient(
    commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

# Create a boto3 client for AWS KMS
kms_client = boto3.client('kms', region_name=aws_region)

# Optional: Create an encryption context
encryption_context: Dict[str, str] = {
    "encryption": "context",
    "is not": "secret",
    "but adds": "useful metadata",
    "that can help you": "be confident that",
    "the data you are handling": "is what you think it is",
}
```

```
# Instantiate the material providers
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create the AWS KMS discovery keyring
discovery_keyring_input: CreateAwsKmsDiscoveryKeyringInput =
 CreateAwsKmsDiscoveryKeyringInput(
    kms_client=kms_client,
    discovery_filter=DiscoveryFilter(
        account_ids=[aws_account_id],
        partition="aws"
    )
)

discovery_keyring: IKeyring = mat_prov.create_aws_kms_discovery_keyring(
    input=discovery_keyring_input
)
```

Rust

```
// Instantiate the AWS Encryption SDK
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create a AWS KMS client.
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);


// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create discovery filter
let discovery_filter = DiscoveryFilter::builder()
    .account_ids(vec![aws_account_id.to_string()])
    .partition("aws".to_string())
    .build()?;
```

```
// Create the AWS KMS discovery keyring
let discovery_keyring = mpl
    .create_aws_kms_discovery_keyring()
    .kms_client(kms_client.clone())
    .discovery_filter(discovery_filter)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
```

```
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create discovery filter
discoveryFilter := mpltypes.DiscoveryFilter{
    AccountIds: []string{kmsKeyAccountID},
    Partition:  "aws",
}
awsKmsDiscoveryKeyringInput := mpltypes.CreateAwsKmsDiscoveryKeyringInput{
    KmsClient:       kmsClient,
    DiscoveryFilter: &discoveryFilter,
}
awsKmsDiscoveryKeyring, err :=
 matProv.CreateAwsKmsDiscoveryKeyring(context.Background(),
 awsKmsDiscoveryKeyringInput)
if err != nil {
    panic(err)
}
```

Menggunakan AWS KMS keyring penemuan regional

Keyring penemuan AWS KMS regional adalah keyring yang tidak menentukan kunci ARNs KMS. Sebaliknya, ini memungkinkan AWS Encryption SDK untuk mendekripsi hanya menggunakan kunci KMS pada khususnya. Wilayah AWS

Saat mendekripsi dengan keyring penemuan AWS KMS regional, AWS Encryption SDK mendekripsi kunci data terenkripsi apa pun yang dienkripsi di bawah yang ditentukan. AWS KMS key Wilayah AWS Agar berhasil, penelepon harus memiliki `kms:Decrypt` izin setidaknya satu dari yang AWS KMS keys ditentukan Wilayah AWS yang mengenkripsi kunci data.

Seperti keyrings penemuan lainnya, keyring penemuan regional tidak berpengaruh pada enkripsi. Ini hanya berfungsi saat mendekripsi pesan terenkripsi. Jika Anda menggunakan keyring penemuan

regional dalam multi-keyring yang digunakan untuk mengenkripsi dan mendekripsi, ini hanya efektif saat mendekripsi. Jika Anda menggunakan keyring penemuan Multi-wilayah untuk mengenkripsi data, sendiri atau dalam multi-keyring, operasi enkripsi gagal.

> **Important**
>
> Jika Anda menyertakan keyring penemuan AWS KMS regional dalam multi-keyring dekripsi, keyring penemuan regional mengesampingkan semua batasan kunci KMS yang ditentukan oleh gantungan kunci lain di multi-keyring. Multi-keyring berperilaku seperti keyring yang paling tidak membatasi. Keyring AWS KMS penemuan tidak berpengaruh pada enkripsi saat digunakan sendiri atau dalam multi-keyring.

Penemuan regional keyring dalam AWS Encryption SDK for C upaya untuk mendekripsi hanya dengan kunci KMS di Wilayah yang ditentukan. Saat Anda menggunakan keyring penemuan di AWS Encryption SDK for JavaScript dan AWS Encryption SDK untuk.NET, Anda mengonfigurasi Wilayah pada AWS KMS klien. AWS Encryption SDK Implementasi ini tidak memfilter kunci KMS berdasarkan Wilayah, tetapi AWS KMS akan gagal dalam permintaan dekripsi untuk kunci KMS di luar Wilayah yang ditentukan.

Jika Anda menggunakan keyring penemuan, sebaiknya gunakan filter penemuan untuk membatasi kunci KMS yang digunakan dalam dekripsi ke kunci yang ditentukan dan partisi. Akun AWS Filter penemuan didukung dalam versi 1.7. x dan kemudian AWS Encryption SDK.

Misalnya, kode berikut membuat keyring penemuan AWS KMS regional dengan filter penemuan. Gantungan kunci ini membatasi kunci KMS di akun 111122223333 di Wilayah AS Barat (Oregon) (us-west-2). AWS Encryption SDK

C

Untuk melihat keyring ini, dan `create_kms_client` metodenya, dalam contoh kerja, lihat kms_discovery.cpp.

```
std::shared_ptr<KmsKeyring::DiscoveryFilter> discovery_filter(
    KmsKeyring::DiscoveryFilter::Builder("aws")
        .AddAccount("111122223333")
        .Build());

struct aws_cryptosdk_keyring *kms_regional_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder()
```

```
 .WithKmsClient(create_kms_client(Aws::Region::US_WEST_2)).BuildDiscovery(discovery_filter))
```

C# / .NET

The AWS Encryption SDK for .NET tidak memiliki keyring penemuan regional khusus. Namun, Anda dapat menggunakan beberapa teknik untuk membatasi kunci KMS yang digunakan saat mendekripsi ke Wilayah tertentu.

Cara paling efisien untuk membatasi Wilayah dalam keyring penemuan adalah dengan menggunakan keyring multi-Region-aware penemuan, meskipun Anda mengenkripsi data hanya menggunakan kunci Wilayah tunggal. Saat menemukan tombol Single-region, multi-Region-aware keyring tidak menggunakan fitur Multi-region apa pun.

Gantungan kunci yang dikembalikan oleh `CreateAwsKmsMrkDiscoveryKeyring()` metode menyaring kunci KMS menurut Wilayah sebelum memanggil. AWS KMS Ini mengirimkan permintaan dekripsi AWS KMS hanya ketika kunci data terenkripsi dienkripsi oleh kunci KMS di Wilayah yang ditentukan oleh parameter dalam objek. `Region` `CreateAwsKmsMrkDiscoveryKeyringInput`

Contoh berikut menggunakan versi 4. x dari AWS Encryption SDK untuk .NET.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

List<string> account = new List<string> { "111122223333" };

// Create the discovery filter
var filter = DiscoveryFilter = new DiscoveryFilter
{
    AccountIds = account,
    Partition = "aws"
};

var regionalDiscoveryKeyringInput = new CreateAwsKmsMrkDiscoveryKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(RegionEndpoint.USWest2),
    Region = RegionEndpoint.USWest2,
    DiscoveryFilter = filter
};
```

```
var kmsRegionalDiscoveryKeyring =
 mpl.CreateAwsKmsMrkDiscoveryKeyring(regionalDiscoveryKeyringInput);
```

Anda juga dapat membatasi kunci KMS ke kunci tertentu Wilayah AWS dengan menentukan Region dalam instance AWS KMS klien Anda () AmazonKeyManagementServiceClient. Namun, konfigurasi ini kurang efisien dan berpotensi lebih mahal daripada menggunakan keyring multi-Region-aware penemuan. Alih-alih memfilter kunci KMS berdasarkan Wilayah sebelum menelepon AWS KMS, AWS Encryption SDK untuk .NET memanggil AWS KMS setiap kunci data terenkripsi (hingga mendekripsi satu) dan bergantung pada AWS KMS untuk membatasi kunci KMS yang digunakannya ke Wilayah yang ditentukan.

Contoh berikut menggunakan versi 4. x dari AWS Encryption SDK untuk .NET.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

List<string> account = new List<string> { "111122223333" };

// Create the discovery filter,
// but not a AWS KMS key
var createRegionalDiscoveryKeyringInput = new CreateAwsKmsDiscoveryKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(RegionEndpoint.USWest2),
    DiscoveryFilter = new DiscoveryFilter()
    {
        AccountIds = account,
        Partition = "aws"
    }
};

var kmsRegionalDiscoveryKeyring =
 mlp.CreateAwsKmsDiscoveryKeyring(createRegionalDiscoveryKeyringInput);
```

JavaScript Browser

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

```
import {
```

```
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const clientProvider = getClient(KMS, { credentials })

const discovery = true
const clientProvider = limitRegions(['us-west-2'], getKmsClient)
const keyring = new KmsKeyringBrowser(clientProvider, {
    discovery,
    discoveryFilter: { accountIDs: ['111122223333'], partition: 'aws' }
})
```

JavaScript Node.js

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

Untuk melihat keyring ini, dan `limitRegions` fungsinya, dalam contoh kerja, lihat kms_regional_discovery.ts.

```
import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const discovery = true
const clientProvider = limitRegions(['us-west-2'], getKmsClient)
const keyring = new KmsKeyringNode({
    clientProvider,
    discovery,
```

```
    discoveryFilter: { accountIDs: ['111122223333'], partition: 'aws' }
})
```

Java

```
// Create the discovery filter
DiscoveryFilter discoveryFilter = DiscoveryFilter.builder()
        .partition("aws")
        .accountIds(111122223333)
        .build();
// Create the discovery keyring
CreateAwsKmsMrkDiscoveryMultiKeyringInput createAwsKmsMrkDiscoveryMultiKeyringInput
 = CreateAwsKmsMrkDiscoveryMultiKeyringInput.builder()
        .discoveryFilter(discoveryFilter)
        .regions("us-west-2")
        .build();
IKeyring decryptKeyring =
 matProv.CreateAwsKmsMrkDiscoveryMultiKeyring(createAwsKmsMrkDiscoveryMultiKeyringInput);
```

Python

```
# Instantiate the AWS Encryption SDK
client = aws_encryption_sdk.EncryptionSDKClient(
    commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

# Create a boto3 client for AWS KMS
kms_client = boto3.client('kms', region_name=aws_region)

# Optional: Create an encryption context
encryption_context: Dict[str, str] = {
    "encryption": "context",
    "is not": "secret",
    "but adds": "useful metadata",
    "that can help you": "be confident that",
    "the data you are handling": "is what you think it is",
}

# Instantiate the material providers
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)
```

```
# Create the AWS KMS regional discovery keyring
regional_discovery_keyring_input: CreateAwsKmsMrkDiscoveryKeyringInput = \
    CreateAwsKmsMrkDiscoveryKeyringInput(
        kms_client=kms_client,
        region=mrk_replica_decrypt_region,
        discovery_filter=DiscoveryFilter(
            account_ids=[111122223333],
            partition="aws"
        )
)

    regional_discovery_keyring: IKeyring =
 mat_prov.create_aws_kms_mrk_discovery_keyring(
        input=regional_discovery_keyring_input
    )
```

Rust

```
// Instantiate the AWS Encryption SDK
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Optional: Create an encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create an AWS KMS client
let decrypt_kms_config = aws_sdk_kms::config::Builder::from(&sdk_config)
    .region(Region::new(mrk_replica_decrypt_region.clone()))
    .build();
let decrypt_kms_client = aws_sdk_kms::Client::from_conf(decrypt_kms_config);
```

```
// Create discovery filter
let discovery_filter = DiscoveryFilter::builder()
    .account_ids(vec![aws_account_id.to_string()])
    .partition("aws".to_string())
    .build()?;

// Create the regional discovery keyring
let discovery_keyring = mpl
    .create_aws_kms_mrk_discovery_keyring()
    .kms_client(decrypt_kms_client)
    .region(mrk_replica_decrypt_region)
    .discovery_filter(discovery_filter)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
```

```
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Create discovery filter
discoveryFilter := mpltypes.DiscoveryFilter{
    AccountIds: []string{awsAccountID},
    Partition:  "aws",
}

// Create the regional discovery keyring
awsKmsMrkDiscoveryInput := mpltypes.CreateAwsKmsMrkDiscoveryKeyringInput{
    KmsClient:       kmsClient,
    Region:          alternateRegionMrkKeyRegion,
    DiscoveryFilter: &discoveryFilter,
}
awsKmsMrkDiscoveryKeyring, err :=
 matProv.CreateAwsKmsMrkDiscoveryKeyring(context.Background(),
 awsKmsMrkDiscoveryInput)
if err != nil {
    panic(err)
}
```

AWS Encryption SDK for JavaScript Juga mengekspor `excludeRegions` fungsi untuk Node.js dan browser. Fungsi ini menciptakan keyring penemuan AWS KMS regional yang menghilangkan AWS KMS keys di wilayah tertentu. Contoh berikut membuat keyring penemuan AWS KMS regional yang dapat digunakan AWS KMS keys di akun 111122223333 di setiap Wilayah AWS kecuali untuk US East (Virginia N.) (us-east-1).

AWS Encryption SDK for C Tidak memiliki metode analog, tetapi Anda dapat menerapkannya dengan membuat kustom. ClientSupplier

Contoh ini menunjukkan kode untuk Node.js.

```
const discovery = true
const clientProvider = excludeRegions(['us-east-1'], getKmsClient)
const keyring = new KmsKeyringNode({
    clientProvider,
    discovery,
    discoveryFilter: { accountIDs: [111122223333], partition: 'aws' }
})
```

AWS KMS Gantungan kunci hierarkis

Dengan keyring AWS KMS Hierarkis, Anda dapat melindungi materi kriptografi Anda di bawah kunci KMS enkripsi simetris tanpa menelepon AWS KMS setiap kali Anda mengenkripsi atau mendekripsi data. Ini adalah pilihan yang baik untuk aplikasi yang perlu meminimalkan panggilan ke AWS KMS, dan aplikasi yang dapat menggunakan kembali beberapa materi kriptografi tanpa melanggar persyaratan keamanan mereka.

Hierarchical keyring adalah solusi caching materi kriptografi yang mengurangi jumlah AWS KMS panggilan dengan menggunakan kunci cabang yang AWS KMS dilindungi yang disimpan dalam tabel Amazon DynamoDB, dan kemudian secara lokal menyimpan materi kunci cabang yang digunakan dalam operasi enkripsi dan dekripsi. Tabel DynamoDB berfungsi sebagai penyimpanan kunci yang mengelola dan melindungi kunci cabang. Ini menyimpan kunci cabang aktif dan semua versi sebelumnya dari kunci cabang. Kunci cabang aktif adalah versi kunci cabang terbaru. Keyring Hierarkis menggunakan kunci data unik untuk mengenkripsi setiap pesan dan mengenkripsi setiap kunci enkripsi data untuk setiap permintaan enkripsi dan mengenkripsi setiap kunci enkripsi data dengan kunci pembungkus unik yang berasal dari kunci cabang aktif. Keyring Hierarkis tergantung pada hierarki yang ditetapkan antara kunci cabang aktif dan kunci pembungkus turunannya.

Keyring Hierarkis biasanya menggunakan setiap versi kunci cabang untuk memenuhi beberapa permintaan. Tetapi Anda mengontrol sejauh mana kunci cabang aktif digunakan kembali dan menentukan seberapa sering kunci cabang aktif diputar. Versi aktif dari kunci cabang tetap aktif sampai Anda memutarnya. Versi sebelumnya dari kunci cabang aktif tidak akan digunakan untuk melakukan operasi enkripsi, tetapi masih dapat ditanyakan dan digunakan dalam operasi dekripsi.

Ketika Anda membuat instance keyring Hierarchical, itu membuat cache lokal. Anda menentukan batas cache yang menentukan jumlah waktu maksimum materi kunci cabang disimpan dalam cache lokal sebelum kedaluwarsa dan dikeluarkan dari cache. Hierarchical keyring membuat satu AWS

KMS panggilan untuk mendekripsi kunci cabang dan merakit materi kunci cabang saat pertama kali a `branch-key-id` ditentukan dalam suatu operasi. Kemudian, materi kunci cabang disimpan dalam cache lokal dan digunakan kembali untuk semua operasi enkripsi dan dekripsi yang menentukan itu `branch-key-id` sampai batas cache berakhir. Menyimpan materi kunci cabang di cache lokal mengurangi AWS KMS panggilan. Misalnya, pertimbangkan batas cache 15 menit. Jika Anda melakukan 10.000 operasi enkripsi dalam batas cache tersebut, AWS KMS keyring tradisional perlu melakukan 10.000 AWS KMS panggilan untuk memenuhi 10.000 operasi enkripsi. Jika Anda memiliki satu aktif`branch-key-id`, keyring Hierarkis hanya perlu membuat satu AWS KMS panggilan untuk memenuhi 10.000 operasi enkripsi.

Cache lokal memisahkan bahan enkripsi dari bahan dekripsi. Materi enkripsi dirakit dari kunci cabang aktif dan digunakan kembali untuk semua operasi enkripsi hingga batas cache berakhir. Materi dekripsi dirakit dari ID kunci cabang dan versi yang diidentifikasi dalam metadata bidang terenkripsi, dan digunakan kembali untuk semua operasi dekripsi yang terkait dengan ID kunci cabang dan versi hingga batas cache berakhir. Cache lokal dapat menyimpan beberapa versi kunci cabang yang sama sekaligus. Ketika cache lokal dikonfigurasi untuk menggunakan abranch key ID supplier, itu juga dapat menyimpan materi kunci cabang dari beberapa kunci cabang aktif pada satu waktu.

> **Note**
>
> Semua penyebutan keyring Hierarkis AWS Encryption SDK mengacu pada keyring Hierarkis. AWS KMS

Kompatibilitas bahasa pemrograman

Keyring Hierarkis didukung oleh bahasa dan versi pemrograman berikut:

- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK untuk .NET
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi MPL opsional.
- Versi 1. x dari AWS Encryption SDK untuk Rust
- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Topik

- Cara kerjanya
- Prasyarat

- Izin yang diperlukan
- Pilih cache
- Buat keyring Hierarkis

Cara kerjanya

Panduan berikut menjelaskan bagaimana keyring Hierarkis merakit bahan enkripsi dan dekripsi, dan panggilan berbeda yang dibuat oleh keyring untuk mengenkripsi dan mendekripsi operasi. Untuk detail teknis tentang derivasi kunci pembungkus dan proses enkripsi kunci data plaintext, lihat Detail teknis keyring AWS KMS hierarkis.

Enkripsi dan tandatangani

Panduan berikut menjelaskan bagaimana keyring Hierarkis merakit bahan enkripsi dan memperoleh kunci pembungkus yang unik.

1. Metode enkripsi meminta keyring Hierarkis untuk materi enkripsi. Keyring menghasilkan kunci data plaintext, lalu memeriksa untuk melihat apakah ada materi cabang yang valid di cache lokal untuk menghasilkan kunci pembungkus. Jika ada materi kunci cabang yang valid, keyring dilanjutkan ke Langkah 4.
2. Jika tidak ada materi kunci cabang yang valid, keyring Hierarkis menanyakan penyimpanan kunci untuk kunci cabang aktif.

    a. Key store memanggil AWS KMS untuk mendekripsi kunci cabang aktif dan mengembalikan kunci cabang aktif plaintext. Data yang mengidentifikasi kunci cabang aktif diserialisasi untuk memberikan data otentikasi tambahan (AAD) dalam panggilan dekripsi ke. AWS KMS

    b. Toko kunci mengembalikan kunci cabang plaintext dan data yang mengidentifikasinya, seperti versi kunci cabang.
3. Hierarchical keyring merakit materi kunci cabang (kunci cabang plaintext dan versi kunci cabang) dan menyimpan salinannya di cache lokal.
4. Keyring Hierarchical memperoleh kunci pembungkus unik dari kunci cabang plaintext dan garam acak 16-byte. Ini menggunakan kunci pembungkus turunan untuk mengenkripsi salinan kunci data teks biasa.

Metode enkripsi menggunakan bahan enkripsi untuk mengenkripsi data. Untuk informasi selengkapnya, lihat Cara AWS Encryption SDK mengenkripsi data.

Dekripsi dan verifikasi

Panduan berikut menjelaskan bagaimana keyring Hierarkis merakit bahan dekripsi dan mendekripsi kunci data terenkripsi.

1. Metode dekripsi mengidentifikasi kunci data terenkripsi dari pesan terenkripsi, dan meneruskannya ke keyring Hierarkis.
2. Hierarchical keyring deserialisasi data yang mengidentifikasi kunci data terenkripsi, termasuk versi kunci cabang, garam 16-byte, dan informasi lain yang menjelaskan bagaimana kunci data dienkripsi.

   Untuk informasi selengkapnya, lihat AWS KMS Rincian teknis keyring hierarkis.
3. Keyring hierarkis memeriksa untuk melihat apakah ada materi kunci cabang yang valid di cache lokal yang cocok dengan versi kunci cabang yang diidentifikasi pada Langkah 2. Jika ada materi kunci cabang yang valid, keyring dilanjutkan ke Langkah 6.
4. Jika tidak ada materi kunci cabang yang valid, keyring Hierarkis menanyakan penyimpanan kunci untuk kunci cabang yang cocok dengan versi kunci cabang yang diidentifikasi pada Langkah 2.

   a. Key store memanggil AWS KMS untuk mendekripsi kunci cabang dan mengembalikan kunci cabang aktif plaintext. Data yang mengidentifikasi kunci cabang aktif diserialisasi untuk memberikan data otentikasi tambahan (AAD) dalam panggilan dekripsi ke. AWS KMS

   b. Toko kunci mengembalikan kunci cabang plaintext dan data yang mengidentifikasinya, seperti versi kunci cabang.
5. Hierarchical keyring merakit materi kunci cabang (kunci cabang plaintext dan versi kunci cabang) dan menyimpan salinannya di cache lokal.
6. Keyring Hierarchical menggunakan bahan kunci cabang yang dirakit dan garam 16-byte yang diidentifikasi pada Langkah 2 untuk mereproduksi kunci pembungkus unik yang mengenkripsi kunci data.
7. Keyring Hierarkis menggunakan kunci pembungkus yang direproduksi untuk mendekripsi kunci data dan mengembalikan kunci data plaintext.

Metode dekripsi menggunakan bahan dekripsi dan kunci data teks biasa untuk mendekripsi pesan terenkripsi. Untuk informasi selengkapnya, lihat Cara AWS Encryption SDK mendekripsi pesan terenkripsi.

Prasyarat

Sebelum Anda membuat dan menggunakan keyring Hierarkis, pastikan prasyarat berikut terpenuhi.

- Anda, atau administrator toko kunci Anda, telah membuat toko kunci dan membuat setidaknya satu kunci cabang aktif.
- Anda telah mengonfigurasi tindakan penyimpanan utama Anda.

> **Note**
>
> Cara Anda mengonfigurasi tindakan penyimpanan kunci menentukan operasi apa yang dapat Anda lakukan dan kunci KMS apa yang dapat digunakan oleh keyring Hierarkis. Untuk informasi selengkapnya, lihat Tindakan penyimpanan kunci.

- Anda memiliki AWS KMS izin yang diperlukan untuk mengakses dan menggunakan kunci penyimpanan dan cabang kunci. Untuk informasi selengkapnya, lihat the section called “Izin yang diperlukan”.
- Anda telah meninjau jenis cache yang didukung dan mengonfigurasi jenis cache yang paling sesuai dengan kebutuhan Anda. Untuk informasi selengkapnya, lihat the section called “Pilih cache”

Izin yang diperlukan

AWS Encryption SDK Itu tidak memerlukan Akun AWS dan itu tidak tergantung pada apa pun Layanan AWS. Namun, untuk menggunakan keyring Hierarkis, Anda memerlukan izin minimum Akun AWS dan berikut pada enkripsi simetris di AWS KMS key toko kunci Anda.

- Untuk mengenkripsi dan mendekripsi data dengan keyring Hierarkis, Anda memerlukan KMS: Decrypt.
- Untuk membuat dan memutar kunci cabang, Anda memerlukan kms: GenerateDataKeyWithoutPlaintext dan kms:. ReEncrypt

Untuk informasi selengkapnya tentang mengontrol akses ke kunci cabang dan penyimpanan kunci Anda, lihatthe section called “Menerapkan izin yang paling tidak diistimewakan”.

Pilih cache

Keyring Hierarkis mengurangi jumlah panggilan yang dilakukan AWS KMS dengan menyimpan materi kunci cabang secara lokal yang digunakan dalam operasi enkripsi dan dekripsi. Sebelum Anda membuat keyring Hierarkis Anda, Anda perlu memutuskan jenis cache yang ingin Anda gunakan. Anda dapat menggunakan cache default atau menyesuaikan cache agar sesuai dengan kebutuhan Anda.

Keyring Hierarkis mendukung jenis cache berikut:

- the section called “Cache default”
- the section called “MultiThreaded cache”
- the section called “StormTracking cache”
- the section called “Cache bersama”

> **Important**
>
> Semua jenis cache yang didukung dirancang untuk mendukung lingkungan multithreaded. Namun, ketika digunakan dengan AWS Encryption SDK for Python, keyring Hierarchical tidak mendukung lingkungan multithreaded. Untuk informasi selengkapnya, lihat file Python README.rst di repositori -library pada. aws-cryptographic-material-providers GitHub

Cache default

Untuk sebagian besar pengguna, cache Default memenuhi persyaratan threading mereka. Cache Default dirancang untuk mendukung lingkungan yang sangat multithreaded. Ketika entri materi kunci cabang kedaluwarsa, cache Default mencegah beberapa utas memanggil AWS KMS dengan memberi tahu satu utas bahwa entri materi kunci cabang akan kedaluwarsa 10 detik sebelumnya. Ini memastikan bahwa hanya satu utas yang mengirimkan permintaan AWS KMS untuk menyegarkan cache.

Default dan StormTracking cache mendukung model threading yang sama, tetapi Anda hanya perlu menentukan kapasitas entri untuk menggunakan cache Default. Untuk kustomisasi cache yang lebih terperinci, gunakan file. the section called “StormTracking cache”

Kecuali Anda ingin menyesuaikan jumlah entri materi kunci cabang yang dapat disimpan di cache lokal, Anda tidak perlu menentukan jenis cache saat Anda membuat keyring Hierarkis. Jika Anda

tidak menentukan jenis cache, keyring Hierarkis menggunakan jenis cache Default dan menetapkan kapasitas entri ke 1000.

Untuk menyesuaikan cache Default, tentukan nilai berikut:

- Kapasitas entri: membatasi jumlah entri materi kunci cabang yang dapat disimpan di cache lokal.

Java

```
.cache(CacheType.builder()
        .Default(DefaultCache.builder()
        .entryCapacity(100)
        .build())
```

C# / .NET

```
CacheType defaultCache = new CacheType
{
    Default = new DefaultCache{EntryCapacity = 100}
};
```

Python

```
default_cache = CacheTypeDefault(
    value=DefaultCache(
        entry_capacity=100
    )
)
```

Rust

```
let cache: CacheType = CacheType::Default(
    DefaultCache::builder()
        .entry_capacity(100)
        .build()?,
);
```

Go

```
cache := mpltypes.CacheTypeMemberDefault{
  Value: mpltypes.DefaultCache{
```

```
   EntryCapacity: 100,
  },
 }
```

MultiThreaded cache

MultiThreaded Cache aman digunakan di lingkungan multithreaded, tetapi tidak menyediakan fungsionalitas apa pun untuk meminimalkan atau panggilan Amazon AWS KMS DynamoDB. Akibatnya, ketika entri materi kunci cabang kedaluwarsa, semua utas akan diberitahukan pada saat yang sama. Ini dapat menghasilkan beberapa AWS KMS panggilan untuk menyegarkan cache.

Untuk menggunakan MultiThreaded cache, tentukan nilai berikut:

- Kapasitas entri: membatasi jumlah entri materi kunci cabang yang dapat disimpan di cache lokal.
- Ukuran ekor pemangkasan entri: menentukan jumlah entri yang akan dipangkas jika kapasitas masuk tercapai.

Java

```
.cache(CacheType.builder()
        .MultiThreaded(MultiThreadedCache.builder()
        .entryCapacity(100)
        .entryPruningTailSize(1)
        .build())
```

C# / .NET

```
CacheType multithreadedCache = new CacheType
{
    MultiThreaded = new MultiThreadedCache
    {
        EntryCapacity = 100,
        EntryPruningTailSize = 1
    }
};
```

Python

```
multithreaded_cache = CacheTypeMultiThreaded(
    value=MultiThreadedCache(
```

```
        entry_capacity=100,
        entry_pruning_tail_size=1
    )
)
```

Rust

```
CacheType::MultiThreaded(
            MultiThreadedCache::builder()
                    .entry_capacity(100)
                    .entry_pruning_tail_size(1)
                    .build()?)
```

Go

```
var entryPruningTailSize int32 = 1
 cache := mpltypes.CacheTypeMemberMultiThreaded{
  Value: mpltypes.MultiThreadedCache{
   EntryCapacity:        100,
   EntryPruningTailSize: &entryPruningTailSize,
  },
 }
```

StormTracking cache

StormTracking Cache dirancang untuk mendukung lingkungan yang sangat multithreaded. Ketika entri materi kunci cabang kedaluwarsa, StormTracking cache mencegah beberapa utas memanggil AWS KMS dengan memberi tahu satu utas bahwa entri materi kunci cabang akan kedaluwarsa sebelumnya. Ini memastikan bahwa hanya satu utas yang mengirimkan permintaan AWS KMS untuk menyegarkan cache.

Untuk menggunakan StormTracking cache, tentukan nilai berikut:

- Kapasitas entri: membatasi jumlah entri materi kunci cabang yang dapat disimpan di cache lokal.

  Nilai default: 1000 entri
- Ukuran ekor pemangkasan entri: menentukan jumlah entri bahan kunci cabang untuk dipangkas sekaligus.

  Nilai default: 1 entri

- Masa tenggang: mendefinisikan jumlah detik sebelum kedaluwarsa bahwa upaya untuk menyegarkan materi kunci cabang dilakukan.

  Nilai default: 10 detik

- Interval rahmat: mendefinisikan jumlah detik antara upaya untuk menyegarkan materi kunci cabang.

  Nilai default: 1 detik

- Fan out: mendefinisikan jumlah upaya simultan yang dapat dilakukan untuk menyegarkan materi kunci cabang.

  Nilai default: 20 upaya

- In flight time to live (TTL): mendefinisikan jumlah detik hingga upaya untuk menyegarkan materi kunci cabang habis waktu. Setiap kali cache kembali `NoSuchEntry` sebagai respons terhadap a`GetCacheEntry`, kunci cabang tersebut dianggap dalam penerbangan sampai kunci yang sama ditulis dengan `PutCache` entri.

  Nilai default: 10 detik

- Tidur: mendefinisikan jumlah milidetik yang harus ditidurkan oleh sebuah utas jika `fanOut` terlampaui.

  Nilai default: 20 milidetik

Java

```
.cache(CacheType.builder()
        .StormTracking(StormTrackingCache.builder()
        .entryCapacity(100)
        .entryPruningTailSize(1)
        .gracePeriod(10)
        .graceInterval(1)
        .fanOut(20)
        .inFlightTTL(10)
        .sleepMilli(20)
        .build())
```

C# / .NET

```
CacheType stormTrackingCache = new CacheType
```

```
{
    StormTracking = new StormTrackingCache
    {
        EntryCapacity = 100,
        EntryPruningTailSize = 1,
        FanOut = 20,
        GraceInterval = 1,
        GracePeriod = 10,
        InFlightTTL = 10,
        SleepMilli = 20
    }
};
```

Python

```
storm_tracking_cache = CacheTypeStormTracking(
    value=StormTrackingCache(
        entry_capacity=100,
        entry_pruning_tail_size=1,
        fan_out=20,
        grace_interval=1,
        grace_period=10,
        in_flight_ttl=10,
        sleep_milli=20
    )
)
```

Rust

```
CacheType::StormTracking(
                StormTrackingCache::builder()
                    .entry_capacity(100)
                    .entry_pruning_tail_size(1)
                    .grace_period(10)
                    .grace_interval(1)
                    .fan_out(20)
                    .in_flight_ttl(10)
                    .sleep_milli(20)
                    .build()?)
```

Go

```
var entryPruningTailSize int32 = 1
```

```
cache := mpltypes.CacheTypeMemberStormTracking{
 Value: mpltypes.StormTrackingCache{
  EntryCapacity:        100,
  EntryPruningTailSize: &entryPruningTailSize,
  GraceInterval:        1,
  GracePeriod:          10,
  FanOut:               20,
  InFlightTTL:          10,
  SleepMilli:           20,
 },
}
```

Cache bersama

Secara default, keyring Hierarkis membuat cache lokal baru setiap kali Anda membuat instance keyring. Namun, cache Bersama dapat membantu menghemat memori dengan memungkinkan Anda berbagi cache di beberapa gantungan kunci Hierarkis. Daripada membuat cache materi kriptografi baru untuk setiap keyring Hierarkis yang Anda buat instance, cache Bersama hanya menyimpan satu cache dalam memori, yang dapat digunakan oleh semua gantungan kunci Hierarkis yang mereferensikannya. Cache bersama membantu mengoptimalkan penggunaan memori dengan menghindari duplikasi materi kriptografi di seluruh keyrings. Sebagai gantinya, gantungan kunci Hierarkis dapat mengakses cache dasar yang sama, mengurangi jejak memori secara keseluruhan.

Saat Anda membuat cache Bersama, Anda masih menentukan jenis cache. Anda dapat menentukanthe section called “Cache default”,the section called “MultiThreaded cache”, atau the section called “StormTracking cache” sebagai jenis cache, atau mengganti cache kustom yang kompatibel.

Partisi

Beberapa keyrings Hierarkis dapat menggunakan satu cache Bersama. Saat Anda membuat keyring Hierarkis dengan cache Bersama, Anda dapat menentukan ID partisi opsional. ID partisi membedakan keyring Hierarkis mana yang menulis ke cache. Jika dua keyrings hirarkis mereferensikan ID partisi yang samalogical key store name, dan ID kunci cabang kedua keyrings akan berbagi entri cache yang sama dalam cache. Jika Anda membuat dua gantungan kunci Hierarkis dengan cache Bersama yang sama, tetapi partisi yang berbeda IDs, setiap keyring hanya akan mengakses entri cache dari partisi yang ditunjuk sendiri dalam cache Bersama. Partisi bertindak

sebagai divisi logis dalam cache bersama, memungkinkan setiap keyring Hierarkis beroperasi secara independen pada partisi yang ditunjuk sendiri, tanpa mengganggu data yang disimpan di partisi lain.

Jika Anda bermaksud untuk menggunakan kembali atau berbagi entri cache di partisi, Anda harus menentukan ID partisi Anda sendiri. Saat Anda meneruskan ID partisi ke keyring Hierarkis Anda, keyring dapat menggunakan kembali entri cache yang sudah ada di cache Bersama, daripada harus mengambil dan mengotorisasi ulang materi kunci cabang lagi. Jika Anda tidak menentukan ID partisi, ID partisi unik secara otomatis ditetapkan ke keyring setiap kali Anda membuat instance keyring Hierarkis.

Prosedur berikut menunjukkan cara membuat cache Bersama dengan tipe cache Default dan meneruskannya ke keyring Hierarkis.

1. Buat `CryptographicMaterialsCache` (CMC) menggunakan Material Providers Library (MPL).

   Java

   ```
   // Instantiate the MPL
   final MaterialProviders matProv =
       MaterialProviders.builder()
           .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
           .build();

   // Create a CacheType object for the Default cache
   final CacheType cache =
       CacheType.builder()
           .Default(DefaultCache.builder().entryCapacity(100).build())
           .build();

   // Create a CMC using the default cache
   final CreateCryptographicMaterialsCacheInput cryptographicMaterialsCacheInput =
       CreateCryptographicMaterialsCacheInput.builder()
           .cache(cache)
           .build();

   final ICryptographicMaterialsCache sharedCryptographicMaterialsCache =
       matProv.CreateCryptographicMaterialsCache(cryptographicMaterialsCacheInput);
   ```

   C# / .NET

   ```
   // Instantiate the MPL
   ```

```
var materialProviders = new MaterialProviders(new MaterialProvidersConfig());

// Create a CacheType object for the Default cache
var cache = new CacheType { Default = new DefaultCache{EntryCapacity = 100} };

// Create a CMC using the default cache
var cryptographicMaterialsCacheInput = new
 CreateCryptographicMaterialsCacheInput {Cache = cache};

var sharedCryptographicMaterialsCache =
 materialProviders.CreateCryptographicMaterialsCache(cryptographicMaterialsCacheInput);
```

Python

```
# Instantiate the MPL
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create a CacheType object for the default cache
cache: CacheType = CacheTypeDefault(
    value=DefaultCache(
        entry_capacity=100,
    )
)

# Create a CMC using the default cache
cryptographic_materials_cache_input = CreateCryptographicMaterialsCacheInput(
    cache=cache,
)

shared_cryptographic_materials_cache =
 mat_prov.create_cryptographic_materials_cache(
    cryptographic_materials_cache_input
)
```

Rust

```
// Instantiate the MPL
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create a CacheType object for the default cache
```

```
let cache: CacheType = CacheType::Default(
    DefaultCache::builder()
        .entry_capacity(100)
        .build()?,
);

// Create a CMC using the default cache
let shared_cryptographic_materials_cache: CryptographicMaterialsCacheRef = mpl.
    create_cryptographic_materials_cache()
    .cache(cache)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
)

// Instantiate the MPL
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create a CacheType object for the default cache
cache := mpltypes.CacheTypeMemberDefault{
    Value: mpltypes.DefaultCache{
        EntryCapacity: 100,
    },
}

// Create a CMC using the default cache
cmcCacheInput := mpltypes.CreateCryptographicMaterialsCacheInput{
    Cache: &cache,
}
sharedCryptographicMaterialsCache, err :=
 matProv.CreateCryptographicMaterialsCache(context.Background(), cmcCacheInput)
```

```
if err != nil {
    panic(err)
}
```

2. Buat `CacheType` objek untuk cache Bersama.

   Lulus yang `sharedCryptographicMaterialsCache` Anda buat di Langkah 1 ke `CacheType` objek baru.

   Java

   ```
   // Create a CacheType object for the sharedCryptographicMaterialsCache
   final CacheType sharedCache =
       CacheType.builder()
           .Shared(sharedCryptographicMaterialsCache)
           .build();
   ```

   C# / .NET

   ```
   // Create a CacheType object for the sharedCryptographicMaterialsCache
   var sharedCache = new CacheType { Shared = sharedCryptographicMaterialsCache };
   ```

   Python

   ```
   # Create a CacheType object for the shared_cryptographic_materials_cache
   shared_cache: CacheType = CacheTypeShared(
       value=shared_cryptographic_materials_cache
   )
   ```

   Rust

   ```
   // Create a CacheType object for the shared_cryptographic_materials_cache
   let shared_cache: CacheType =
    CacheType::Shared(shared_cryptographic_materials_cache);
   ```

   Go

   ```
   // Create a CacheType object for the shared_cryptographic_materials_cache
   ```

```
shared_cache :=
 mpltypes.CacheTypeMemberShared{sharedCryptographicMaterialsCache}
```

3. Lewati `sharedCache` objek dari Langkah 2 ke keyring Hierarkis Anda.

Saat Anda membuat keyring Hierarkis dengan cache Bersama, Anda dapat secara opsional menentukan entri `partitionID` untuk berbagi cache di beberapa gantungan kunci Hierarkis. Jika Anda tidak menentukan ID partisi, keyring Hierarkis secara otomatis menetapkan keyring ID partisi unik.

> **Note**
>
> Keyring Hierarkis Anda akan berbagi entri cache yang sama dalam cache Bersama jika Anda membuat dua atau lebih keyrings yang mereferensikan ID partisi yang samalogical key store name, dan ID kunci cabang. Jika Anda tidak ingin beberapa keyrings berbagi entri cache yang sama, Anda harus menggunakan ID partisi unik untuk setiap keyring Hierarkis.

Contoh berikut membuat keyring Hierarkis denganbranch key ID supplier, dan batas cache 600 detik. Untuk informasi selengkapnya tentang nilai yang ditentukan dalam konfigurasi keyring Hierarkis berikut, lihat. the section called “Buat keyring Hierarkis”

Java

```
// Create the Hierarchical keyring
final CreateAwsKmsHierarchicalKeyringInput keyringInput =
    CreateAwsKmsHierarchicalKeyringInput.builder()
        .keyStore(keystore)
        .branchKeyIdSupplier(branchKeyIdSupplier)
        .ttlSeconds(600)
        .cache(sharedCache)
        .partitionID(partitionID)
        .build();
final IKeyring hierarchicalKeyring =
 matProv.CreateAwsKmsHierarchicalKeyring(keyringInput);
```

C# / .NET

```
// Create the Hierarchical keyring
```

```
var createKeyringInput = new CreateAwsKmsHierarchicalKeyringInput
{
   KeyStore = keystore,
   BranchKeyIdSupplier = branchKeyIdSupplier,
   Cache = sharedCache,
   TtlSeconds = 600,
   PartitionId = partitionID
};
var keyring =
 materialProviders.CreateAwsKmsHierarchicalKeyring(createKeyringInput);
```

Python

```
# Create the Hierarchical keyring
keyring_input: CreateAwsKmsHierarchicalKeyringInput =
 CreateAwsKmsHierarchicalKeyringInput(
    key_store=keystore,
    branch_key_id_supplier=branch_key_id_supplier,
    ttl_seconds=600,
    cache=shared_cache,
    partition_id=partition_id
)

hierarchical_keyring: IKeyring = mat_prov.create_aws_kms_hierarchical_keyring(
    input=keyring_input
)
```

Rust

```
// Create the Hierarchical keyring
let keyring1 = mpl
    .create_aws_kms_hierarchical_keyring()
    .key_store(key_store1)
    .branch_key_id(branch_key_id.clone())
    // CryptographicMaterialsCacheRef is an Rc (Reference Counted), so if you
 clone it to
    // pass it to different Hierarchical Keyrings, it will still point to the
 same
    // underlying cache, and increment the reference count accordingly.
    .cache(shared_cache.clone())
    .ttl_seconds(600)
    .partition_id(partition_id.clone())
    .send()
```

```
    .await?;
```

Go

```
// Create the Hierarchical keyring
hkeyringInput := mpltypes.CreateAwsKmsHierarchicalKeyringInput{
    KeyStore:    keyStore1,
    BranchKeyId: &branchKeyId,
    TtlSeconds:  600,
    Cache:       &shared_cache,
    PartitionId: &partitionId,
}
keyring, err := matProv.CreateAwsKmsHierarchicalKeyring(context.Background(),
 hkeyringInput)
if err != nil {
    panic(err)
}
```

Buat keyring Hierarkis

Untuk membuat keyring Hierarkis, Anda harus memberikan nilai-nilai berikut:

- Nama toko kunci

  Nama tabel DynamoDB yang Anda, atau administrator toko utama Anda, dibuat untuk berfungsi sebagai toko kunci Anda.

-

  Batas waktu cache untuk hidup (TTL)

  Jumlah waktu dalam hitungan detik entri materi kunci cabang dalam cache lokal dapat digunakan sebelum kedaluwarsa. Batas cache TTL menentukan seberapa sering klien memanggil AWS KMS untuk mengotorisasi penggunaan kunci cabang. Nilai ini harus lebih besar dari nol. Setelah batas cache TTL berakhir, entri tidak pernah disajikan, dan akan diusir dari cache lokal.

- Pengidentifikasi kunci cabang

  Anda dapat mengonfigurasi secara statis `branch-key-id` yang mengidentifikasi satu kunci cabang aktif di toko kunci Anda, atau memberikan pemasok ID kunci cabang.

Pemasok ID kunci cabang menggunakan bidang yang disimpan dalam konteks enkripsi untuk menentukan kunci cabang mana yang diperlukan untuk mendekripsi catatan.

Kami sangat menyarankan menggunakan pemasok ID kunci cabang untuk database multitenant di mana setiap penyewa memiliki kunci cabang mereka sendiri. Anda dapat menggunakan pemasok ID kunci cabang untuk membuat nama ramah untuk kunci cabang Anda IDs agar mudah mengenali ID kunci cabang yang benar untuk penyewa tertentu. Misalnya, nama ramah memungkinkan Anda merujuk ke kunci cabang sebagai `tenant1` gantinya`ab3f61619-4d35-48ad-a275-050f87e15122`.

Untuk operasi dekripsi, Anda dapat mengonfigurasi secara statis satu keyring Hierarkis untuk membatasi dekripsi ke penyewa tunggal, atau Anda dapat menggunakan pemasok ID kunci cabang untuk mengidentifikasi penyewa mana yang bertanggung jawab untuk mendekripsi catatan.

- (Opsional) Sebuah cache

  Jika Anda ingin menyesuaikan jenis cache atau jumlah entri materi kunci cabang yang dapat disimpan di cache lokal, tentukan jenis cache dan kapasitas entri saat Anda menginisialisasi keyring.

  Keyring Hierarkis mendukung jenis cache berikut: Default,, MultiThreaded StormTracking, dan Shared. Untuk informasi selengkapnya dan contoh yang menunjukkan cara menentukan setiap jenis cache, lihatthe section called “Pilih cache”.

  Jika Anda tidak menentukan cache, keyring Hierarkis secara otomatis menggunakan jenis cache Default dan menetapkan kapasitas entri ke 1000.

- (Opsional) ID partisi

  Jika Anda menentukanthe section called “Cache bersama”, Anda dapat secara opsional menentukan ID partisi. ID partisi membedakan keyring Hierarkis mana yang menulis ke cache. Jika Anda bermaksud untuk menggunakan kembali atau berbagi entri cache di partisi, Anda harus menentukan ID partisi Anda sendiri. Anda dapat menentukan string apa pun untuk ID partisi. Jika Anda tidak menentukan ID partisi, ID partisi unik secara otomatis ditetapkan ke keyring saat pembuatan.

  Untuk informasi selengkapnya, lihat Partitions.

> **Note**
>
> Keyring Hierarkis Anda akan berbagi entri cache yang sama dalam cache Bersama jika Anda membuat dua atau lebih keyrings yang mereferensikan ID partisi yang samalogical key store name, dan ID kunci cabang. Jika Anda tidak ingin beberapa keyrings berbagi entri cache yang sama, Anda harus menggunakan ID partisi unik untuk setiap keyring Hierarkis.

- (Opsional) Daftar Token Hibah

  Jika Anda mengontrol akses ke kunci KMS di keyring Hierarkis Anda dengan hibah, Anda harus menyediakan semua token hibah yang diperlukan saat Anda menginisialisasi keyring.

Buat keyring Hierarkis dengan ID kunci cabang statis

Contoh berikut menunjukkan cara membuat keyring Hierarki dengan ID kunci cabang statis, TTLthe section called “Cache default”, dan batas cache 600 detik.

Java

```
final MaterialProviders matProv = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();
final CreateAwsKmsHierarchicalKeyringInput keyringInput =
 CreateAwsKmsHierarchicalKeyringInput.builder()
        .keyStore(branchKeyStoreName)
        .branchKeyId(branch-key-id)
        .ttlSeconds(600)
        .build();
final Keyring hierarchicalKeyring =
 matProv.CreateAwsKmsHierarchicalKeyring(keyringInput);
```

C# / .NET

```
var matProv = new MaterialProviders(new MaterialProvidersConfig());
var keyringInput = new CreateAwsKmsHierarchicalKeyringInput
{
   KeyStore = keystore,
   BranchKeyId = branch-key-id,
   TtlSeconds = 600
```

```
};
var hierarchicalKeyring = matProv.CreateAwsKmsHierarchicalKeyring(keyringInput);
```

Python

```
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

keyring_input: CreateAwsKmsHierarchicalKeyringInput =
 CreateAwsKmsHierarchicalKeyringInput(
    key_store=keystore,
    branch_key_id=branch_key_id,
    ttl_seconds=600
)

hierarchical_keyring: IKeyring = mat_prov.create_aws_kms_hierarchical_keyring(
    input=keyring_input
)
```

Rust

```
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

let hierarchical_keyring = mpl
        .create_aws_kms_hierarchical_keyring()
        .key_store(key_store.clone())
        .branch_key_id(branch_key_id)
        .ttl_seconds(600)
        .send()
        .await?;
```

Go

```
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}
hkeyringInput := mpltypes.CreateAwsKmsHierarchicalKeyringInput{
    KeyStore:    keyStore,
    BranchKeyId: &branchKeyID,
```

```
    TtlSeconds:  600,
}
hKeyRing, err := matProv.CreateAwsKmsHierarchicalKeyring(context.Background(),
 hkeyringInput)
if err != nil {
    panic(err)
}
```

Buat keyring Hierarkis dengan pemasok ID kunci cabang

Prosedur berikut menunjukkan cara membuat keyring Hierarkis dengan pemasok ID kunci cabang.

1. Buat pemasok ID kunci cabang

   Contoh berikut membuat nama ramah untuk dua kunci cabang dan panggilan `CreateDynamoDbEncryptionBranchKeyIdSupplier` untuk membuat pemasok ID kunci cabang.

   Java

   ```
   // Create friendly names for each branch-key-id
   class ExampleBranchKeyIdSupplier implements IDynamoDbKeyBranchKeyIdSupplier {
       private static String branchKeyIdForTenant1;
       private static String branchKeyIdForTenant2;

       public ExampleBranchKeyIdSupplier(String tenant1Id, String tenant2Id) {
           this.branchKeyIdForTenant1 = tenant1Id;
           this.branchKeyIdForTenant2 = tenant2Id;
       }
   // Create the branch key ID supplier
   final DynamoDbEncryption ddbEnc = DynamoDbEncryption.builder()
           .DynamoDbEncryptionConfig(DynamoDbEncryptionConfig.builder().build())
           .build();
   final BranchKeyIdSupplier branchKeyIdSupplier =
    ddbEnc.CreateDynamoDbEncryptionBranchKeyIdSupplier(
       CreateDynamoDbEncryptionBranchKeyIdSupplierInput.builder()
               .ddbKeyBranchKeyIdSupplier(new ExampleBranchKeyIdSupplier(branch-
   key-ID-tenant1, branch-key-ID-tenant2))
               .build()).branchKeyIdSupplier();
   ```

C# / .NET

```
// Create friendly names for each branch-key-id
 class ExampleBranchKeyIdSupplier : DynamoDbKeyBranchKeyIdSupplierBase {
    private String _branchKeyIdForTenant1;
    private String _branchKeyIdForTenant2;

    public ExampleBranchKeyIdSupplier(String tenant1Id, String tenant2Id) {
        this._branchKeyIdForTenant1 = tenant1Id;
        this._branchKeyIdForTenant2 = tenant2Id;
    }
// Create the branch key ID supplier
var ddbEnc = new DynamoDbEncryption(new DynamoDbEncryptionConfig());
var branchKeyIdSupplier = ddbEnc.CreateDynamoDbEncryptionBranchKeyIdSupplier(
    new CreateDynamoDbEncryptionBranchKeyIdSupplierInput
    {
        DdbKeyBranchKeyIdSupplier = new ExampleBranchKeyIdSupplier(branch-key-
ID-tenant1, branch-key-ID-tenant2)
    }).BranchKeyIdSupplier;
```

Python

```
# Create branch key ID supplier that maps the branch key ID to a friendly name
branch_key_id_supplier: IBranchKeyIdSupplier = ExampleBranchKeyIdSupplier(
        tenant_1_id=branch_key_id_a,
        tenant_2_id=branch_key_id_b,
)
```

Rust

```
// Create branch key ID supplier that maps the branch key ID to a friendly name
let branch_key_id_supplier = ExampleBranchKeyIdSupplier::new(
    &branch_key_id_a,
    &branch_key_id_b
);
```

Go

```
// Create branch key ID supplier that maps the branch key ID to a friendly name
keySupplier := branchKeySupplier{branchKeyA: branchKeyA, branchKeyB: branchKeyB}
```

2. Buat keyring Hierarkis

Contoh berikut menginisialisasi keyring Hierarkis dengan pemasok ID kunci cabang yang dibuat pada Langkah 1, batas cache TLL 600 detik, dan ukuran cache maksimum 1000.

Java

```
final MaterialProviders matProv = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();
final CreateAwsKmsHierarchicalKeyringInput keyringInput =
 CreateAwsKmsHierarchicalKeyringInput.builder()
        .keyStore(keystore)
        .branchKeyIdSupplier(branchKeyIdSupplier)
        .ttlSeconds(600)
        .cache(CacheType.builder() //OPTIONAL
                .Default(DefaultCache.builder()
                .entryCapacity(100)
                .build())
        .build();
final Keyring hierarchicalKeyring =
 matProv.CreateAwsKmsHierarchicalKeyring(keyringInput);
```

C# / .NET

```
var matProv = new MaterialProviders(new MaterialProvidersConfig());
var keyringInput = new CreateAwsKmsHierarchicalKeyringInput
{
   KeyStore = keystore,
   BranchKeyIdSupplier = branchKeyIdSupplier,
   TtlSeconds = 600,
   Cache = new CacheType
   {
        Default = new DefaultCache { EntryCapacity = 100 }
   }
};
var hierarchicalKeyring = matProv.CreateAwsKmsHierarchicalKeyring(keyringInput);
```

Python

```
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
```

```
)

keyring_input: CreateAwsKmsHierarchicalKeyringInput =
 CreateAwsKmsHierarchicalKeyringInput(
    key_store=keystore,
    branch_key_id_supplier=branch_key_id_supplier,
    ttl_seconds=600,
    cache=CacheTypeDefault(
        value=DefaultCache(
            entry_capacity=100
        )
    ),
)

hierarchical_keyring: IKeyring = mat_prov.create_aws_kms_hierarchical_keyring(
    input=keyring_input
)
```

Rust

```
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

let hierarchical_keyring = mpl
    .create_aws_kms_hierarchical_keyring()
    .key_store(key_store.clone())
    .branch_key_id_supplier(branch_key_id_supplier)
    .ttl_seconds(600)
    .send()
    .await?;
```

Go

```
hkeyringInput := mpltypes.CreateAwsKmsHierarchicalKeyringInput{
    KeyStore:            keyStore,
    BranchKeyIdSupplier: &keySupplier,
    TtlSeconds:          600,
}
hKeyRing, err := matProv.CreateAwsKmsHierarchicalKeyring(context.Background(),
 hkeyringInput)
if err != nil {
    panic(err)
```

```
}
```

AWS KMS Gantungan kunci ECDH

Gantungan kunci AWS KMS ECDH menggunakan kesepakatan kunci asimetris AWS KMS keysuntuk mendapatkan kunci pembungkus simetris bersama antara dua pihak. Pertama, keyring menggunakan algoritma perjanjian kunci Elliptic Curve Diffie-Hellman (ECDH) untuk mendapatkan rahasia bersama dari kunci pribadi di KMS key pair pengirim dan kunci publik penerima. Kemudian, keyring menggunakan rahasia bersama untuk mendapatkan kunci pembungkus bersama yang melindungi kunci enkripsi data Anda. Fungsi derivasi kunci yang AWS Encryption SDK digunakan (`KDF_CTR_HMAC_SHA384`) untuk menurunkan kunci pembungkus bersama sesuai dengan rekomendasi NIST untuk derivasi kunci.

Fungsi derivasi kunci mengembalikan 64 byte bahan kunci. Untuk memastikan bahwa kedua belah pihak menggunakan materi kunci yang benar, AWS Encryption SDK menggunakan 32 byte pertama sebagai kunci komitmen dan 32 byte terakhir sebagai kunci pembungkus bersama. Saat mendekripsi, jika keyring tidak dapat mereproduksi kunci komitmen yang sama dan kunci pembungkus bersama yang disimpan di ciphertext header pesan, operasi gagal. Misalnya, jika Anda mengenkripsi data dengan keyring yang dikonfigurasi dengan kunci pribadi Alice dan kunci publik Bob, keyring yang dikonfigurasi dengan kunci pribadi Bob dan kunci publik Alice akan mereproduksi kunci komitmen yang sama dan kunci pembungkus bersama dan dapat mendekripsi data. Jika kunci publik Bob bukan dari key pair KMS, maka Bob dapat membuat keyring ECDH mentah untuk mendekripsi data.

Keyring AWS KMS ECDH mengenkripsi data dengan kunci simetris menggunakan AES-GCM. Kunci data kemudian dienkripsi dengan kunci pembungkus bersama turunan menggunakan AES-GCM. Setiap keyring AWS KMS ECDH hanya dapat memiliki satu kunci pembungkus bersama, tetapi Anda dapat menyertakan beberapa gantungan kunci AWS KMS ECDH, sendiri atau dengan gantungan kunci lainnya, dalam multi-keyring.

Kompatibilitas bahasa pemrograman

Keyring AWS KMS ECDH diperkenalkan dalam versi 1.5.0 dari Cryptographic Material Providers Library (MPL) dan didukung oleh bahasa dan versi pemrograman berikut:

- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK untuk .NET
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi MPL opsional.

- Versi 1. x dari AWS Encryption SDK untuk Rust
- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Topik

Izin yang diperlukan untuk gantungan kunci AWS KMS ECDH

AWS Encryption SDK Tidak memerlukan AWS akun dan tidak tergantung pada AWS layanan apa pun. Namun, untuk menggunakan keyring AWS KMS ECDH, Anda memerlukan AWS akun dan izin minimum berikut pada keyring Anda. AWS KMS keys Izin bervariasi berdasarkan skema perjanjian kunci yang Anda gunakan.

- Untuk mengenkripsi dan mendekripsi data menggunakan skema perjanjian `KmsPrivateKeyToStaticPublicKey` kunci, Anda memerlukan kms: GetPublicKey dan kms: DeriveSharedSecret pada key pair KMS asimetris pengirim. Jika Anda langsung memberikan kunci publik yang dienkode DER pengirim saat membuat instance keyring, Anda hanya perlu DeriveSharedSecret izin kms: pada key pair KMS asimetris pengirim.
- Untuk mendekripsi data menggunakan skema perjanjian `KmsPublicKeyDiscovery` kunci, Anda memerlukan GetPublicKey izin kms: DeriveSharedSecret dan kms: pada key pair KMS asimetris yang ditentukan.

Membuat keyring AWS KMS ECDH

Untuk membuat keyring AWS KMS ECDH yang mengenkripsi dan mendekripsi data, Anda harus menggunakan skema perjanjian kunci. `KmsPrivateKeyToStaticPublicKey`
Untuk menginisialisasi keyring AWS KMS ECDH dengan skema perjanjian `KmsPrivateKeyToStaticPublicKey` kunci, berikan nilai-nilai berikut:

- ID Pengirim AWS KMS key

  Harus mengidentifikasi asymmetric NIST recommended elliptic curve (ECC) KMS key pair dengan nilai. `KeyUsage` `KEY_AGREEMENT` Kunci pribadi pengirim digunakan untuk mendapatkan rahasia bersama.

- (Opsional) Kunci publik pengirim

  Harus berupa kunci publik X.509 yang dikodekan DER, juga dikenal sebagai `SubjectPublicKeyInfo` (SPKI), sebagaimana didefinisikan dalam RFC 5280.

  AWS KMS GetPublicKeyOperasi mengembalikan kunci publik dari key pair KMS asimetris dalam format yang dienkode DER yang diperlukan.

  Untuk mengurangi jumlah AWS KMS panggilan yang dilakukan keyring Anda, Anda dapat langsung memberikan kunci publik pengirim. Jika tidak ada nilai yang diberikan untuk kunci publik pengirim, keyring akan memanggil AWS KMS untuk mengambil kunci publik pengirim.

- Kunci publik penerima

  Anda harus memberikan kunci publik X.509 yang dikodekan DER penerima, juga dikenal sebagai `SubjectPublicKeyInfo` (SPKI), sebagaimana didefinisikan dalam RFC 5280.

  AWS KMS GetPublicKeyOperasi mengembalikan kunci publik dari key pair KMS asimetris dalam format yang dienkode DER yang diperlukan.

- Spesifikasi kurva

  Mengidentifikasi spesifikasi kurva elips dalam pasangan kunci yang ditentukan. Pasangan kunci pengirim dan penerima harus memiliki spesifikasi kurva yang sama.

  Nilai valid: `ECC_NIST_P256`, `ECC_NIS_P384`, `ECC_NIST_P512`

- (Opsional) Daftar Token Hibah

  Jika Anda mengontrol akses ke kunci KMS di keyring AWS KMS ECDH Anda dengan hibah, Anda harus memberikan semua token hibah yang diperlukan saat Anda menginisialisasi keyring.

C# / .NET

Contoh berikut membuat keyring AWS KMS ECDH dengan kunci KMS pengirim, kunci publik pengirim, dan kunci publik penerima. Contoh ini menggunakan `SenderPublicKey` parameter opsional untuk menyediakan kunci publik pengirim. Jika Anda tidak memberikan kunci publik pengirim, keyring akan memanggil AWS KMS untuk mengambil kunci publik pengirim. Pasangan kunci pengirim dan penerima berada di `ECC_NIST_P256` kurva.

```
// Instantiate material providers
var materialProviders = new MaterialProviders(new MaterialProvidersConfig());
```

```
// Must be DER-encoded X.509 public keys
var BobPublicKey = new MemoryStream(new byte[] { });
var AlicePublicKey = new MemoryStream(new byte[] { });

// Create the AWS KMS ECDH static keyring
var staticConfiguration = new KmsEcdhStaticConfigurations
{
    KmsPrivateKeyToStaticPublicKey = new KmsPrivateKeyToStaticPublicKeyInput
    {
        SenderKmsIdentifier = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        SenderPublicKey = BobPublicKey,
        RecipientPublicKey = AlicePublicKey
    }
};

var createKeyringInput = new CreateAwsKmsEcdhKeyringInput
{
    CurveSpec = ECDHCurveSpec.ECC_NIST_P256,
    KmsClient = new AmazonKeyManagementServiceClient(),
    KeyAgreementScheme = staticConfiguration
};

var keyring = materialProviders.CreateAwsKmsEcdhKeyring(createKeyringInput);
```

Java

Contoh berikut membuat keyring AWS KMS ECDH dengan kunci KMS pengirim, kunci publik pengirim, dan kunci publik penerima. Contoh ini menggunakan `senderPublicKey` parameter opsional untuk menyediakan kunci publik pengirim. Jika Anda tidak memberikan kunci publik pengirim, keyring akan memanggil AWS KMS untuk mengambil kunci publik pengirim. Pasangan kunci pengirim dan penerima berada di `ECC_NIST_P256` kurva.

```
// Retrieve public keys
// Must be DER-encoded X.509 public keys
ByteBuffer BobPublicKey = getPublicKeyBytes("arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab");
        ByteBuffer AlicePublicKey = getPublicKeyBytes("arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321");

// Create the AWS KMS ECDH static keyring
        final CreateAwsKmsEcdhKeyringInput senderKeyringInput =
```

```
            CreateAwsKmsEcdhKeyringInput.builder()
              .kmsClient(KmsClient.create())
              .curveSpec(ECDHCurveSpec.ECC_NIST_P256)
              .KeyAgreementScheme(
                KmsEcdhStaticConfigurations.builder()
                  .KmsPrivateKeyToStaticPublicKey(
                    KmsPrivateKeyToStaticPublicKeyInput.builder()
                      .senderKmsIdentifier("arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab")
                      .senderPublicKey(BobPublicKey)
                      .recipientPublicKey(AlicePublicKey)
                      .build()).build()).build();
```

Python

Contoh berikut membuat keyring AWS KMS ECDH dengan kunci KMS pengirim, kunci publik pengirim, dan kunci publik penerima. Contoh ini menggunakan `senderPublicKey` parameter opsional untuk menyediakan kunci publik pengirim. Jika Anda tidak memberikan kunci publik pengirim, keyring akan memanggil AWS KMS untuk mengambil kunci publik pengirim. Pasangan kunci pengirim dan penerima berada di `ECC_NIST_P256` kurva.

```
import boto3
from aws_cryptographic_materialproviders.mpl.models import (
    CreateAwsKmsEcdhKeyringInput,
    KmsEcdhStaticConfigurationsKmsPrivateKeyToStaticPublicKey,
    KmsPrivateKeyToStaticPublicKeyInput,
)
from aws_cryptography_primitives.smithygenerated.aws_cryptography_primitives.models
 import ECDHCurveSpec

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Retrieve public keys
# Must be DER-encoded X.509 public keys
bob_public_key = get_public_key_bytes("arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab")
alice_public_key = get_public_key_bytes("arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321")

# Create the AWS KMS ECDH static keyring
```

```
sender_keyring_input = CreateAwsKmsEcdhKeyringInput(
    kms_client = boto3.client('kms', region_name="us-west-2"),
    curve_spec = ECDHCurveSpec.ECC_NIST_P256,
    key_agreement_scheme =
 KmsEcdhStaticConfigurationsKmsPrivateKeyToStaticPublicKey(
        KmsPrivateKeyToStaticPublicKeyInput(
            sender_kms_identifier = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            sender_public_key = bob_public_key,
            recipient_public_key = alice_public_key,

        )
    )
)

keyring = mat_prov.create_aws_kms_ecdh_keyring(sender_keyring_input)
```

Rust

Contoh berikut membuat keyring AWS KMS ECDH dengan kunci KMS pengirim, kunci publik pengirim, dan kunci publik penerima. Contoh ini menggunakan `sender_public_key` parameter opsional untuk menyediakan kunci publik pengirim. Jika Anda tidak memberikan kunci publik pengirim, keyring akan memanggil AWS KMS untuk mengambil kunci publik pengirim.

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create the AWS KMS client
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Optional: Create your encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);
```

```
// Retrieve public keys
// Must be DER-encoded X.509 keys
let public_key_file_content_sender =
 std::fs::read_to_string(Path::new(EXAMPLE_KMS_ECC_PUBLIC_KEY_FILENAME_SENDER))?;
let parsed_public_key_file_content_sender = parse(public_key_file_content_sender)?;
let public_key_sender_utf8_bytes = parsed_public_key_file_content_sender.contents();

let public_key_file_content_recipient =
 std::fs::read_to_string(Path::new(EXAMPLE_KMS_ECC_PUBLIC_KEY_FILENAME_RECIPIENT))?;
let parsed_public_key_file_content_recipient =
 parse(public_key_file_content_recipient)?;
let public_key_recipient_utf8_bytes =
 parsed_public_key_file_content_recipient.contents();

// Create KmsPrivateKeyToStaticPublicKeyInput
let kms_ecdh_static_configuration_input =
    KmsPrivateKeyToStaticPublicKeyInput::builder()
        .sender_kms_identifier(arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab)
        // Must be a UTF8 DER-encoded X.509 public key
        .sender_public_key(public_key_sender_utf8_bytes)
        // Must be a UTF8 DER-encoded X.509 public key
        .recipient_public_key(public_key_recipient_utf8_bytes)
        .build()?;

let kms_ecdh_static_configuration =
 KmsEcdhStaticConfigurations::KmsPrivateKeyToStaticPublicKey(kms_ecdh_static_configuration_i

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create AWS KMS ECDH keyring
let kms_ecdh_keyring = mpl
    .create_aws_kms_ecdh_keyring()
    .kms_client(kms_client)
    .curve_spec(ecdh_curve_spec)
    .key_agreement_scheme(kms_ecdh_static_configuration)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Retrieve public keys
// Must be DER-encoded X.509 keys
publicKeySender, err := utils.LoadPublicKeyFromPEM(kmsEccPublicKeyFileNameSender)
```

```
if err != nil {
    panic(err)
}
publicKeyRecipient, err :=
 utils.LoadPublicKeyFromPEM(kmsEccPublicKeyFileNameRecipient)
if err != nil {
    panic(err)
}

// Create KmsPrivateKeyToStaticPublicKeyInput
kmsEcdhStaticConfigurationInput := mpltypes.KmsPrivateKeyToStaticPublicKeyInput{
    RecipientPublicKey:  publicKeyRecipient,
    SenderKmsIdentifier: arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab,
    SenderPublicKey:     publicKeySender,
}
kmsEcdhStaticConfiguration :=
 &mpltypes.KmsEcdhStaticConfigurationsMemberKmsPrivateKeyToStaticPublicKey{
    Value: kmsEcdhStaticConfigurationInput,
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create AWS KMS ECDH keyring
awsKmsEcdhKeyringInput := mpltypes.CreateAwsKmsEcdhKeyringInput{
    CurveSpec:          ecdhCurveSpec,
    KeyAgreementScheme: kmsEcdhStaticConfiguration,
    KmsClient:          kmsClient,
}
awsKmsEcdhKeyring, err := matProv.CreateAwsKmsEcdhKeyring(context.Background(),
 awsKmsEcdhKeyringInput)
if err != nil {
    panic(err)
}
```

Membuat keyring AWS KMS penemuan ECDH

Saat mendekripsi, ini adalah praktik terbaik untuk menentukan kunci yang AWS Encryption SDK dapat digunakan. Untuk mengikuti praktik terbaik ini, gunakan gantungan kunci AWS KMS ECDH dengan skema perjanjian `KmsPrivateKeyToStaticPublicKey` kunci. Namun, Anda juga dapat membuat keyring penemuan AWS KMS ECDH, yaitu keyring AWS KMS ECDH yang dapat mendekripsi pesan apa pun di mana kunci publik dari key pair KMS yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

> **Important**
>
> Ketika Anda mendekripsi pesan menggunakan skema perjanjian `KmsPublicKeyDiscovery` kunci, Anda menerima semua kunci publik, terlepas dari siapa yang memilikinya.

Untuk menginisialisasi keyring AWS KMS ECDH dengan skema perjanjian `KmsPublicKeyDiscovery` kunci, berikan nilai-nilai berikut:

- AWS KMS key ID Penerima

  Harus mengidentifikasi asymmetric NIST recommended elliptic curve (ECC) KMS key pair dengan nilai. `KeyUsage` `KEY_AGREEMENT`
- Spesifikasi kurva

  Mengidentifikasi spesifikasi kurva eliptik dalam key pair KMS penerima.

  Nilai valid: `ECC_NIST_P256`, `ECC_NIS_P384`, `ECC_NIST_P512`
- (Opsional) Daftar Token Hibah

  Jika Anda mengontrol akses ke kunci KMS di keyring AWS KMS ECDH Anda dengan hibah, Anda harus memberikan semua token hibah yang diperlukan saat Anda menginisialisasi keyring.

C# / .NET

Contoh berikut membuat keyring penemuan AWS KMS ECDH dengan key pair KMS pada kurva. `ECC_NIST_P256` Anda harus memiliki DeriveSharedSecret izin kms: GetPublicKey dan kms: pada key pair KMS yang ditentukan. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari key pair KMS yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
// Instantiate material providers
var materialProviders = new MaterialProviders(new MaterialProvidersConfig());

// Create the AWS KMS ECDH discovery keyring
var discoveryConfiguration = new KmsEcdhStaticConfigurations
{
    KmsPublicKeyDiscovery = new KmsPublicKeyDiscoveryInput
    {
        RecipientKmsIdentifier = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    }

};
var createKeyringInput = new CreateAwsKmsEcdhKeyringInput
{
    CurveSpec = ECDHCurveSpec.ECC_NIST_P256,
    KmsClient = new AmazonKeyManagementServiceClient(),
    KeyAgreementScheme = discoveryConfiguration
};
var keyring = materialProviders.CreateAwsKmsEcdhKeyring(createKeyringInput);
```

Java

Contoh berikut membuat keyring penemuan AWS KMS ECDH dengan key pair KMS pada kurva. ECC_NIST_P256 Anda harus memiliki DeriveSharedSecret izin kms: GetPublicKey dan kms: pada key pair KMS yang ditentukan. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari key pair KMS yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
// Create the AWS KMS ECDH discovery keyring
final CreateAwsKmsEcdhKeyringInput recipientKeyringInput =
  CreateAwsKmsEcdhKeyringInput.builder()
    .kmsClient(KmsClient.create())
    .curveSpec(ECDHCurveSpec.ECC_NIST_P256)
    .KeyAgreementScheme(
      KmsEcdhStaticConfigurations.builder()
        .KmsPublicKeyDiscovery(
          KmsPublicKeyDiscoveryInput.builder()
            .recipientKmsIdentifier("arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321").build()
        ).build())
    .build();
```

Python

Contoh berikut membuat keyring penemuan AWS KMS ECDH dengan key pair KMS pada kurva. `ECC_NIST_P256` Anda harus memiliki DeriveSharedSecret izin kms: GetPublicKey dan kms: pada key pair KMS yang ditentukan. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari key pair KMS yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
import boto3
from aws_cryptographic_materialproviders.mpl.models import (
    CreateAwsKmsEcdhKeyringInput,
    KmsEcdhStaticConfigurationsKmsPublicKeyDiscovery,
    KmsPublicKeyDiscoveryInput,
)
from aws_cryptography_primitives.smithygenerated.aws_cryptography_primitives.models
 import ECDHCurveSpec

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create the AWS KMS ECDH discovery keyring
create_keyring_input = CreateAwsKmsEcdhKeyringInput(
    kms_client = boto3.client('kms', region_name="us-west-2"),
    curve_spec = ECDHCurveSpec.ECC_NIST_P256,
    key_agreement_scheme = KmsEcdhStaticConfigurationsKmsPublicKeyDiscovery(
        KmsPublicKeyDiscoveryInput(
            recipient_kms_identifier = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
        )
    )
)

keyring = mat_prov.create_aws_kms_ecdh_keyring(create_keyring_input)
```

Rust

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create the AWS KMS client
```

```
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Optional: Create your encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Create KmsPublicKeyDiscoveryInput
let kms_ecdh_discovery_static_configuration_input =
    KmsPublicKeyDiscoveryInput::builder()
        .recipient_kms_identifier(ecc_recipient_key_arn)
        .build()?;

let kms_ecdh_discovery_static_configuration =
 KmsEcdhStaticConfigurations::KmsPublicKeyDiscovery(kms_ecdh_discovery_static_configuration_

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create AWS KMS ECDH discovery keyring
let kms_ecdh_discovery_keyring = mpl
    .create_aws_kms_ecdh_keyring()
    .kms_client(kms_client.clone())
    .curve_spec(ecdh_curve_spec)
    .key_agreement_scheme(kms_ecdh_discovery_static_configuration)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
```

```
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Create KmsPublicKeyDiscoveryInput
kmsEcdhDiscoveryStaticConfigurationInput := mpltypes.KmsPublicKeyDiscoveryInput{
    RecipientKmsIdentifier: eccRecipientKeyArn,
}
kmsEcdhDiscoveryStaticConfiguration :=
 &mpltypes.KmsEcdhStaticConfigurationsMemberKmsPublicKeyDiscovery{
    Value: kmsEcdhDiscoveryStaticConfigurationInput,
}

// Instantiate the material providers library
```

```
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create AWS KMS ECDH discovery keyring
awsKmsEcdhDiscoveryKeyringInput := mpltypes.CreateAwsKmsEcdhKeyringInput{
    CurveSpec:          ecdhCurveSpec,
    KeyAgreementScheme: kmsEcdhDiscoveryStaticConfiguration,
    KmsClient:          kmsClient,
}
awsKmsEcdhDiscoveryKeyring, err :=
 matProv.CreateAwsKmsEcdhKeyring(context.Background(),
 awsKmsEcdhDiscoveryKeyringInput)
if err != nil {
    panic(err)
}
```

Gantungan kunci AES mentah

Ini AWS Encryption SDK memungkinkan Anda menggunakan kunci simetris AES yang Anda berikan sebagai kunci pembungkus yang melindungi kunci data Anda. Anda perlu membuat, menyimpan, dan melindungi materi utama, sebaiknya dalam modul keamanan perangkat keras (HSM) atau sistem manajemen kunci. Gunakan keyring Raw AES saat Anda perlu memberikan kunci pembungkus dan mengenkripsi kunci data secara lokal atau offline.

Raw AES keyring mengenkripsi data dengan menggunakan algoritma AES-GCM dan kunci pembungkus yang Anda tentukan sebagai array byte. Anda hanya dapat menentukan satu kunci pembungkus di setiap keyring Raw AES, tetapi Anda dapat menyertakan beberapa gantungan kunci Raw AES, sendiri atau dengan gantungan kunci lainnya, dalam multi-keyring.

Raw AES keyring setara dengan dan berinteraksi dengan JceMasterKeykelas di AWS Encryption SDK for Java dan RawMasterKeykelas AWS Encryption SDK for Python ketika mereka digunakan dengan kunci enkripsi AES. Anda dapat mengenkripsi data dengan satu implementasi dan mendekripsi data dengan implementasi lain menggunakan kunci pembungkus yang sama. Lihat perinciannya di Kompatibilitas keyring.

Ruang nama dan nama kunci

Untuk mengidentifikasi kunci AES dalam keyring, keyring Raw AES menggunakan namespace kunci dan nama kunci yang Anda berikan. Nilai-nilai ini bukan rahasia. Mereka muncul dalam teks biasa di header pesan terenkripsi yang dikembalikan oleh operasi enkripsi. Sebaiknya gunakan namespace kunci HSM atau sistem manajemen kunci Anda dan nama kunci yang mengidentifikasi kunci AES dalam sistem itu.

> **Note**
>
> Namespace kunci dan nama kunci setara dengan kolom ID Penyedia (atau Penyedia) dan ID Kunci di `JceMasterKey` dan. `RawMasterKey`
> The AWS Encryption SDK for C and AWS Encryption SDK for .NET menyimpan nilai namespace `aws-kms` kunci untuk kunci KMS. Jangan gunakan nilai namespace ini dalam keyring Raw AES atau Raw RSA keyring dengan pustaka ini.

Jika Anda membuat keyring yang berbeda untuk mengenkripsi dan mendekripsi pesan yang diberikan, namespace dan nilai nama sangat penting. Jika namespace kunci dan nama kunci dalam keyring dekripsi bukan kecocokan yang tepat dan peka huruf besar/kecil untuk namespace kunci dan nama kunci dalam keyring enkripsi, keyring dekripsi tidak digunakan, meskipun byte materi kunci identik.

Misalnya, Anda mungkin mendefinisikan keyring Raw AES dengan namespace `HSM_01` kunci dan nama kunci. `AES_256_012` Kemudian, Anda menggunakan keyring itu untuk mengenkripsi beberapa data. Untuk mendekripsi data tersebut, buat keyring Raw AES dengan namespace kunci, nama kunci, dan material kunci yang sama.

Contoh berikut menunjukkan cara membuat keyring Raw AES. `AESWrappingKey`Variabel mewakili materi kunci yang Anda berikan.

C

Untuk membuat instance keyring Raw AES di, gunakan. AWS Encryption SDK for C`aws_cryptosdk_raw_aes_keyring_new()` Untuk contoh lengkap, lihat raw_aes_keyring.c.

```
struct aws_allocator *alloc = aws_default_allocator();

AWS_STATIC_STRING_FROM_LITERAL(wrapping_key_namespace, "HSM_01");
AWS_STATIC_STRING_FROM_LITERAL(wrapping_key_name, "AES_256_012");

struct aws_cryptosdk_keyring *raw_aes_keyring = aws_cryptosdk_raw_aes_keyring_new(
```

```
        alloc, wrapping_key_namespace, wrapping_key_name, aes_wrapping_key,
 wrapping_key_len);
```

C# / .NET

Untuk membuat keyring Raw AES AWS Encryption SDK untuk .NET, gunakan metode in`materialProviders.CreateRawAesKeyring()`. Untuk contoh lengkapnya, lihat Raw AESKeyring Example.cs.

Contoh berikut menggunakan versi 4. x dari AWS Encryption SDK untuk .NET.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

var keyNamespace = "HSM_01";
var keyName = "AES_256_012";

// This example uses the key generator in Bouncy Castle to generate the key
 material.
// In production, use key material from a secure source.
var aesWrappingKey = new
 MemoryStream(GeneratorUtilities.GetKeyGenerator("AES256").GenerateKey());

// Create the keyring that determines how your data keys are protected.
var createKeyringInput = new CreateRawAesKeyringInput
{
    KeyNamespace = keyNamespace,
    KeyName = keyName,
    WrappingKey = aesWrappingKey,
    WrappingAlg = AesWrappingAlg.ALG_AES256_GCM_IV12_TAG16
};

var keyring = materialProviders.CreateRawAesKeyring(createKeyringInput);
```

JavaScript Browser

AWS Encryption SDK for JavaScript Di browser mendapatkan primitif kriptografinya dari API. WebCrypto Sebelum Anda membuat keyring, Anda harus menggunakan `RawAesKeyringWebCrypto.importCryptoKey()` untuk mengimpor bahan kunci mentah ke backend. WebCrypto Ini memastikan bahwa keyring selesai meskipun semua panggilan ke WebCrypto asinkron.

Kemudian, untuk membuat instance keyring Raw AES, gunakan metode ini. `RawAesKeyringWebCrypto()` Anda harus menentukan algoritma pembungkus AES ("wrapping suite) berdasarkan panjang materi kunci Anda. Untuk contoh lengkap, lihat aes_simple.ts (Browser). JavaScript

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called "Membatasi kunci data terenkripsi".

```
import {
  RawAesWrappingSuiteIdentifier,
  RawAesKeyringWebCrypto,
  synchronousRandomValues,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-browser'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const keyNamespace = 'HSM_01'
const keyName = 'AES_256_012'

const wrappingSuite =
  RawAesWrappingSuiteIdentifier.AES256_GCM_IV12_TAG16_NO_PADDING

/* Import the plaintext AES key into the WebCrypto backend. */
const aesWrappingKey = await RawAesKeyringWebCrypto.importCryptoKey(
  rawAesKey,
  wrappingSuite
)

const rawAesKeyring = new RawAesKeyringWebCrypto({
  keyName,
  keyNamespace,
  wrappingSuite,
  aesWrappingKey
})
```

JavaScript Node.js

Untuk membuat instance keyring Raw AES di AWS Encryption SDK for JavaScript untuk Node.js, buat instance kelas. `RawAesKeyringNode` Anda harus menentukan algoritma pembungkus AES ("wrapping suite") berdasarkan panjang materi kunci Anda. Untuk contoh lengkap, lihat aes_simple.ts (Node.js). JavaScript

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called "Membatasi kunci data terenkripsi".

```
import {
  RawAesKeyringNode,
  buildClient,
  CommitmentPolicy,
  RawAesWrappingSuiteIdentifier,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const keyName = 'AES_256_012'
const keyNamespace = 'HSM_01'

const wrappingSuite =
  RawAesWrappingSuiteIdentifier.AES256_GCM_IV12_TAG16_NO_PADDING

const rawAesKeyring = new RawAesKeyringNode({
  keyName,
  keyNamespace,
  aesWrappingKey,
  wrappingSuite,
})
```

Java

Untuk membuat instance keyring Raw AES di, gunakan. AWS Encryption SDK for Java`matProv.CreateRawAesKeyring()`

```
final CreateRawAesKeyringInput keyringInput = CreateRawAesKeyringInput.builder()
```

```
        .keyName("AES_256_012")
        .keyNamespace("HSM_01")
        .wrappingKey(AESWrappingKey)
        .wrappingAlg(AesWrappingAlg.ALG_AES256_GCM_IV12_TAG16)
        .build();
final MaterialProviders matProv = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();
IKeyring rawAesKeyring = matProv.CreateRawAesKeyring(keyringInput);
```

Python

Contoh berikut membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. REQUIRE_ENCRYPT_REQUIRE_DECRYPT Untuk contoh lengkap, lihat raw_aes_keyring_example.py di AWS Encryption SDK for Python repositori di. GitHub

```
# Instantiate the AWS Encryption SDK client
client = aws_encryption_sdk.EncryptionSDKClient(
    commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

# Define the key namespace and key name
key_name_space = "HSM_01"
key_name = "AES_256_012"

# Optional: Create an encryption context
encryption_context: Dict[str, str] = {
    "encryption": "context",
    "is not": "secret",
    "but adds": "useful metadata",
    "that can help you": "be confident that",
    "the data you are handling": "is what you think it is",
}

# Instantiate the material providers
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create Raw AES keyring
keyring_input: CreateRawAesKeyringInput = CreateRawAesKeyringInput(
    key_namespace=key_name_space,
    key_name=key_name,
```

```
    wrapping_key=AESWrappingKey,
    wrapping_alg=AesWrappingAlg.ALG_AES256_GCM_IV12_TAG16
)

raw_aes_keyring: IKeyring = mat_prov.create_raw_aes_keyring(
    input=keyring_input
)
```

Rust

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Define the key namespace and key name
let key_namespace: &str = "HSM_01";
let key_name: &str = "AES_256_012";

// Optional: Create an encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create Raw AES keyring
let raw_aes_keyring = mpl
    .create_raw_aes_keyring()
    .key_name(key_name)
    .key_namespace(key_namespace)
    .wrapping_key(aws_smithy_types::Blob::new(AESWrappingKey))
    .wrapping_alg(AesWrappingAlg::AlgAes256GcmIv12Tag16)
    .send()
    .await?;
```

Go

```
import (
    mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
    client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
    esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)
//Instantiate the AWS Encryption SDK client.
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}
// Define the key namespace and key name
var keyNamespace = "A managed aes keys"
var keyName = "My 256-bit AES wrapping key"

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}
// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}
// Create Raw AES keyring
aesKeyRingInput := mpltypes.CreateRawAesKeyringInput{
    KeyName:      keyName,
    KeyNamespace: keyNamespace,
    WrappingKey:  aesWrappingKey,
    WrappingAlg:  mpltypes.AesWrappingAlgAlgAes256GcmIv12Tag16,
}
aesKeyring, err := matProv.CreateRawAesKeyring(context.Background(),
 aesKeyRingInput)
if err != nil {
```

```
    panic(err)
}
```

Gantungan kunci RSA mentah

Raw RSA keyring melakukan enkripsi asimetris dan dekripsi kunci data dalam memori lokal dengan kunci publik dan pribadi RSA yang Anda berikan. Anda perlu membuat, menyimpan, dan melindungi kunci pribadi, sebaiknya dalam modul keamanan perangkat keras (HSM) atau sistem manajemen kunci. Fungsi enkripsi mengenkripsi kunci data di bawah kunci publik RSA. Fungsi dekripsi mendekripsi kunci data menggunakan kunci pribadi. Anda dapat memilih dari antara beberapa mode padding RSA.

Raw RSA keyring yang mengenkripsi dan mendekripsi harus menyertakan kunci publik asimetris dan private key pair. Namun, Anda dapat mengenkripsi data dengan keyring Raw RSA yang hanya memiliki kunci publik, dan Anda dapat mendekripsi data dengan keyring Raw RSA yang hanya memiliki kunci pribadi. Anda dapat menyertakan keyring Raw RSA apa pun dalam multi-keyring. Jika Anda mengonfigurasi keyring Raw RSA dengan kunci publik dan pribadi, pastikan bahwa mereka adalah bagian dari key pair yang sama. Beberapa implementasi bahasa tidak AWS Encryption SDK akan membangun keyring Raw RSA dengan kunci dari pasangan yang berbeda. Orang lain mengandalkan Anda untuk memverifikasi bahwa kunci Anda berasal dari key pair yang sama.

Raw RSA keyring setara dengan dan berinteraksi dengan in AWS Encryption SDK for Java dan JceMasterKeyin AWS Encryption SDK for Python ketika mereka digunakan dengan kunci enkripsi asimetris RSA. RawMasterKey Anda dapat mengenkripsi data dengan satu implementasi dan mendekripsi data dengan implementasi lain menggunakan kunci pembungkus yang sama. Lihat perinciannya di Kompatibilitas keyring.

> **Note**
>
> Raw RSA keyring tidak mendukung kunci KMS asimetris. Jika Anda ingin menggunakan kunci KMS RSA asimetris, bahasa pemrograman berikut mendukung AWS KMS keyrings yang menggunakan RSA asimetris: AWS KMS keys
>
> - Versi 3. x dari AWS Encryption SDK for Java
> - Versi 4. x dari AWS Encryption SDK untuk .NET
> - Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi Perpustakaan Penyedia Materi Kriptografi (MPL) opsional.

- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Jika Anda mengenkripsi data dengan keyring Raw RSA yang menyertakan kunci publik kunci RSA KMS, baik maupun tidak dapat mendekripsi. AWS Encryption SDK AWS KMS Anda tidak dapat mengekspor kunci pribadi kunci KMS AWS KMS asimetris ke dalam keyring Raw RSA. Operasi AWS KMS Dekripsi tidak dapat mendekripsi pesan terenkripsi yang dikembalikan. AWS Encryption SDK

Saat membuat keyring Raw RSA di AWS Encryption SDK for C, pastikan untuk memberikan konten file PEM yang menyertakan setiap kunci sebagai C-string yang dihentikan nol, bukan sebagai jalur atau nama file. Saat membuat keyring Raw RSA JavaScript, waspadai potensi ketidakcocokan dengan implementasi bahasa lain.

Ruang nama dan nama

Untuk mengidentifikasi materi kunci RSA dalam keyring, keyring Raw RSA menggunakan namespace kunci dan nama kunci yang Anda berikan. Nilai-nilai ini bukan rahasia. Mereka muncul dalam teks biasa di header pesan terenkripsi yang dikembalikan oleh operasi enkripsi. Sebaiknya gunakan namespace kunci dan nama kunci yang mengidentifikasi key pair RSA (atau kunci privatnya) di HSM atau sistem manajemen kunci Anda.

> **Note**
>
> Namespace kunci dan nama kunci setara dengan kolom ID Penyedia (atau Penyedia) dan ID Kunci di `JceMasterKey` dan. `RawMasterKey`
> AWS Encryption SDK for C Cadangan nilai namespace `aws-kms` kunci untuk kunci KMS. Jangan menggunakannya dalam keyring Raw AES atau Raw RSA keyring dengan. AWS Encryption SDK for C

Jika Anda membuat keyring yang berbeda untuk mengenkripsi dan mendekripsi pesan yang diberikan, namespace dan nilai nama sangat penting. Jika namespace kunci dan nama kunci dalam keyring dekripsi bukan kecocokan yang tepat dan peka huruf besar/kecil untuk namespace kunci dan nama kunci dalam keyring enkripsi, keyring dekripsi tidak digunakan, bahkan jika kunci tersebut berasal dari key pair yang sama.

Namespace kunci dan nama kunci dari bahan kunci dalam enkripsi dan dekripsi keyrings harus sama apakah keyring berisi kunci publik RSA, kunci pribadi RSA, atau kedua kunci dalam key pair. Misalnya, Anda mengenkripsi data dengan keyring Raw RSA untuk kunci publik RSA dengan namespace kunci dan nama `HSM_01` kunci. `RSA_2048_06` Untuk mendekripsi data tersebut, buat keyring Raw RSA dengan kunci pribadi (atau key pair), dan namespace dan nama kunci yang sama.

Modus padding

Anda harus menentukan mode padding untuk keyring Raw RSA yang digunakan untuk enkripsi dan dekripsi, atau menggunakan fitur implementasi bahasa Anda yang menentukannya untuk Anda.

AWS Encryption SDK Mendukung mode padding berikut, tunduk pada kendala masing-masing bahasa. Kami merekomendasikan mode padding OAEP, terutama OAEP dengan SHA-256 dan dengan SHA-256 Padding. MGF1 Mode PKCS1padding hanya didukung untuk kompatibilitas mundur.

- OAEP dengan SHA-1 dan MGF1 dengan SHA-1 Padding
- OAEP dengan SHA-256 dan dengan SHA-256 Padding MGF1
- OAEP dengan SHA-384 dan dengan Padding SHA-384 MGF1
- OAEP dengan SHA-512 dan dengan Padding SHA-512 MGF1
- PKCS1 v1.5 Bantalan

Contoh berikut menunjukkan cara membuat keyring Raw RSA dengan kunci publik dan pribadi dari key pair RSA dan OAEP dengan SHA-256 dan dengan mode padding SHA-256. MGF1 `RSAPrivateKey`Variabel `RSAPublicKey` dan mewakili materi kunci yang Anda berikan.

C

Untuk membuat keyring Raw RSA di AWS Encryption SDK for C, gunakan. `aws_cryptosdk_raw_rsa_keyring_new`

Saat membuat keyring Raw RSA di AWS Encryption SDK for C, pastikan untuk memberikan konten file PEM yang menyertakan setiap kunci sebagai C-string yang dihentikan nol, bukan sebagai jalur atau nama file. Untuk contoh lengkap, lihat raw_rsa_keyring.c.

```
struct aws_allocator *alloc = aws_default_allocator();

AWS_STATIC_STRING_FROM_LITERAL(key_namespace, "HSM_01");
```

```
AWS_STATIC_STRING_FROM_LITERAL(key_name, "RSA_2048_06");

struct aws_cryptosdk_keyring *rawRsaKeyring = aws_cryptosdk_raw_rsa_keyring_new(
    alloc,
    key_namespace,
    key_name,
    private_key_from_pem,
    public_key_from_pem,
    AWS_CRYPTOSDK_RSA_OAEP_SHA256_MGF1);
```

C# / .NET

Untuk membuat instance Raw RSA keyring di AWS Encryption SDK for .NET, gunakan metode ini. `materialProviders.CreateRawRsaKeyring()` Untuk contoh lengkapnya, lihat Raw RSAKeyring Example.cs.

Contoh berikut menggunakan versi 4. x dari AWS Encryption SDK untuk .NET.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());

var keyNamespace = "HSM_01";
var keyName = "RSA_2048_06";

// Get public and private keys from PEM files
var publicKey = new
 MemoryStream(System.IO.File.ReadAllBytes("RSAKeyringExamplePublicKey.pem"));
var privateKey = new
 MemoryStream(System.IO.File.ReadAllBytes("RSAKeyringExamplePrivateKey.pem"));

// Create the keyring input
var createRawRsaKeyringInput = new CreateRawRsaKeyringInput
{
    KeyNamespace = keyNamespace,
    KeyName = keyName,
    PaddingScheme = PaddingScheme.OAEP_SHA512_MGF1,
    PublicKey = publicKey,
    PrivateKey = privateKey
};

// Create the keyring
var rawRsaKeyring = materialProviders.CreateRawRsaKeyring(createRawRsaKeyringInput);
```

JavaScript Browser

AWS Encryption SDK for JavaScript Di browser mendapatkan primitif kriptografinya dari perpustakaan. WebCrypto Sebelum Anda membuat keyring, Anda harus menggunakan `importPublicKey()` and/or `importPrivateKey()` untuk mengimpor bahan kunci mentah ke backend. WebCrypto Ini memastikan bahwa keyring selesai meskipun semua panggilan ke WebCrypto asinkron. Objek yang diambil metode impor mencakup algoritma pembungkus dan mode padding-nya.

Setelah mengimpor materi kunci, gunakan `RawRsaKeyringWebCrypto()` metode untuk membuat instance keyring. Saat membuat keyring Raw RSA JavaScript, waspadai potensi ketidakcocokan dengan implementasi bahasa lain.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

Untuk contoh lengkap, lihat rsa_simple.ts (Browser). JavaScript

```
import {
  RsaImportableKey,
  RawRsaKeyringWebCrypto,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-browser'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const privateKey = await RawRsaKeyringWebCrypto.importPrivateKey(
  privateRsaJwKKey
)

const publicKey = await RawRsaKeyringWebCrypto.importPublicKey(
  publicRsaJwKKey
)

const keyNamespace = 'HSM_01'
const keyName = 'RSA_2048_06'
```

```
const keyring = new RawRsaKeyringWebCrypto({
  keyName,
  keyNamespace,
  publicKey,
  privateKey,
})
```

JavaScript Node.js

Untuk membuat instance Raw RSA keyring AWS Encryption SDK for JavaScript untuk Node.js, buat instance baru dari kelas. `RawRsaKeyringNode` `wrapKey`Parameter memegang kunci publik. `unwrapKey`Parameter memegang kunci pribadi. `RawRsaKeyringNode`Konstruktor menghitung mode padding default untuk Anda, meskipun Anda dapat menentukan mode padding yang disukai.

Saat membuat keyring RSA mentah JavaScript, waspadai potensi ketidakcocokan dengan implementasi bahasa lain.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

Untuk contoh lengkap, lihat rsa_simple.ts (Node.js). JavaScript

```
import {
  RawRsaKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const keyNamespace = 'HSM_01'
const keyName = 'RSA_2048_06'

const keyring = new RawRsaKeyringNode({ keyName, keyNamespace, rsaPublicKey,
 rsaPrivateKey})
```

Java

```
final CreateRawRsaKeyringInput keyringInput = CreateRawRsaKeyringInput.builder()
        .keyName("RSA_2048_06")
        .keyNamespace("HSM_01")
        .paddingScheme(PaddingScheme.OAEP_SHA256_MGF1)
        .publicKey(RSAPublicKey)
        .privateKey(RSAPrivateKey)
        .build();
final MaterialProviders matProv = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();
IKeyring rawRsaKeyring = matProv.CreateRawRsaKeyring(keyringInput);
```

Python

Contoh berikut membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. REQUIRE_ENCRYPT_REQUIRE_DECRYPT Untuk contoh lengkap, lihat raw_rsa_keyring_example.py di AWS Encryption SDK for Python repositori di. GitHub

```
# Define the key namespace and key name
key_name_space = "HSM_01"
key_name = "RSA_2048_06"

# Instantiate the material providers
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Create Raw RSA keyring
keyring_input: CreateRawRsaKeyringInput = CreateRawRsaKeyringInput(
    key_namespace=key_name_space,
    key_name=key_name,
    padding_scheme=PaddingScheme.OAEP_SHA256_MGF1,
    public_key=RSAPublicKey,
    private_key=RSAPrivateKey
)

raw_rsa_keyring: IKeyring = mat_prov.create_raw_rsa_keyring(
    input=keyring_input
)
```

Rust

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Optional: Create an encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Define the key namespace and key name
let key_namespace: &str = "HSM_01";
let key_name: &str = "RSA_2048_06";

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create Raw RSA keyring
let raw_rsa_keyring = mpl
    .create_raw_rsa_keyring()
    .key_name(key_name)
    .key_namespace(key_namespace)
    .padding_scheme(PaddingScheme::OaepSha256Mgf1)
    .public_key(aws_smithy_types::Blob::new(RSAPublicKey))
    .private_key(aws_smithy_types::Blob::new(RSAPrivateKey))
    .send()
    .await?;
```

Go

```
// Instantiate the material providers library
matProv, err :=
 awscryptographymaterialproviderssmithygenerated.NewClient(awscryptographymaterialproviderss

// Create Raw RSA keyring
```

```
rsaKeyRingInput :=
 awscryptographymaterialproviderssmithygeneratedtypes.CreateRawRsaKeyringInput{
 KeyName:       "rsa",
 KeyNamespace:  "rsa-keyring",
 PaddingScheme:
 awscryptographymaterialproviderssmithygeneratedtypes.PaddingSchemePkcs1,
 PublicKey:     pem.EncodeToMemory(publicKeyBlock),
 PrivateKey:    pem.EncodeToMemory(privateKeyBlock),
}

rsaKeyring, err := matProv.CreateRawRsaKeyring(context.Background(),
 rsaKeyRingInput)
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}
```

```
// Define the key namespace and key name
var keyNamespace = "HSM_01"
var keyName = "RSA_2048_06"

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create Raw RSA keyring
rsaKeyRingInput := mpltypes.CreateRawRsaKeyringInput{
    KeyName:       keyName,
    KeyNamespace:  keyNamespace,
    PaddingScheme: mpltypes.PaddingSchemeOaepSha512Mgf1,
    PublicKey:     (RSAPublicKey),
    PrivateKey:    (RSAPrivateKey),
}
rsaKeyring, err := matProv.CreateRawRsaKeyring(context.Background(),
 rsaKeyRingInput)
if err != nil {
    panic(err)
}
```

Gantungan kunci ECDH mentah

Raw ECDH keyring menggunakan kurva elips pasangan kunci publik-pribadi yang Anda berikan untuk mendapatkan kunci pembungkus bersama antara dua pihak. Pertama, keyring memperoleh rahasia bersama menggunakan kunci pribadi pengirim, kunci publik penerima, dan algoritma perjanjian kunci Elliptic Curve Diffie-Hellman (ECDH). Kemudian, keyring menggunakan rahasia bersama untuk mendapatkan kunci pembungkus bersama yang melindungi kunci enkripsi data Anda. Fungsi derivasi kunci yang AWS Encryption SDK digunakan (`KDF_CTR_HMAC_SHA384`) untuk menurunkan kunci pembungkus bersama sesuai dengan rekomendasi NIST untuk derivasi kunci.

Fungsi derivasi kunci mengembalikan 64 byte bahan kunci. Untuk memastikan bahwa kedua belah pihak menggunakan materi kunci yang benar, AWS Encryption SDK menggunakan 32 byte pertama sebagai kunci komitmen dan 32 byte terakhir sebagai kunci pembungkus bersama. Saat mendekripsi, jika keyring tidak dapat mereproduksi kunci komitmen yang sama dan kunci pembungkus bersama yang disimpan di ciphertext header pesan, operasi gagal. Misalnya, jika Anda mengenkripsi data

dengan keyring yang dikonfigurasi dengan kunci pribadi Alice dan kunci publik Bob, keyring yang dikonfigurasi dengan kunci pribadi Bob dan kunci publik Alice akan mereproduksi kunci komitmen yang sama dan kunci pembungkus bersama dan dapat mendekripsi data. Jika kunci publik Bob berasal dari AWS KMS key pasangan, maka Bob dapat membuat keyring AWS KMS ECDH untuk mendekripsi data.

Raw ECDH keyring mengenkripsi data dengan kunci simetris menggunakan AES-GCM. Kunci data kemudian dienkripsi dengan kunci pembungkus bersama turunan menggunakan AES-GCM. Setiap keyring ECDH mentah hanya dapat memiliki satu kunci pembungkus bersama, tetapi Anda dapat menyertakan beberapa gantungan kunci ECDH mentah, sendiri atau dengan gantungan kunci lainnya, dalam multi-keyring.

Anda bertanggung jawab untuk membuat, menyimpan, dan melindungi kunci pribadi Anda, sebaiknya dalam modul keamanan perangkat keras (HSM) atau sistem manajemen kunci. Pasangan kunci pengirim dan penerima banyak berada pada kurva elips yang sama. AWS Encryption SDK Mendukung spesifikasi kurva elips berikut:

- `ECC_NIST_P256`
- `ECC_NIST_P384`
- `ECC_NIST_P512`

Kompatibilitas bahasa pemrograman

Raw ECDH keyring diperkenalkan dalam versi 1.5.0 dari Cryptographic Material Providers Library (MPL) dan didukung oleh bahasa dan versi pemrograman berikut:

- Versi 3. x dari AWS Encryption SDK for Java
- Versi 4. x dari AWS Encryption SDK untuk .NET
- Versi 4. x dari AWS Encryption SDK for Python, bila digunakan dengan dependensi MPL opsional.
- Versi 1. x dari AWS Encryption SDK untuk Rust
- Versi 0.1. x atau yang lebih baru AWS Encryption SDK untuk Go

Membuat keyring ECDH mentah

Raw ECDH keyring mendukung tiga skema perjanjian utama:`RawPrivateKeyToStaticPublicKey`,, dan. `EphemeralPrivateKeyToStaticPublicKey` `PublicKeyDiscovery` Skema perjanjian utama

yang Anda pilih menentukan operasi kriptografi mana yang dapat Anda lakukan dan bagaimana bahan kunci dirakit.

Topik

- RawPrivateKeyToStaticPublicKey
- EphemeralPrivateKeyToStaticPublicKey
- PublicKeyDiscovery

RawPrivateKeyToStaticPublicKey

Gunakan skema perjanjian `RawPrivateKeyToStaticPublicKey` kunci untuk mengonfigurasi kunci pribadi pengirim dan kunci publik penerima secara statis di keyring. Skema perjanjian kunci ini dapat mengenkripsi dan mendekripsi data.

Untuk menginisialisasi keyring ECDH mentah dengan skema perjanjian `RawPrivateKeyToStaticPublicKey` kunci, berikan nilai-nilai berikut:

- Kunci pribadi pengirim

  Anda harus memberikan kunci pribadi yang dikodekan PEM pengirim (PrivateKeyInfo struktur PKCS #8), seperti yang didefinisikan dalam RFC 5958.

- Kunci publik penerima

  Anda harus memberikan kunci publik X.509 yang dikodekan DER penerima, juga dikenal sebagai `SubjectPublicKeyInfo` (SPKI), sebagaimana didefinisikan dalam RFC 5280.

  Anda dapat menentukan kunci publik dari perjanjian kunci asimetris KMS key pair atau kunci publik dari key pair yang dihasilkan di luar. AWS

- Spesifikasi kurva

  Mengidentifikasi spesifikasi kurva elips dalam pasangan kunci yang ditentukan. Pasangan kunci pengirim dan penerima harus memiliki spesifikasi kurva yang sama.

  Nilai valid: `ECC_NIST_P256`, `ECC_NIS_P384`, `ECC_NIST_P512`

C# / .NET

```
// Instantiate material providers
```

```
var materialProviders = new MaterialProviders(new MaterialProvidersConfig());
     var BobPrivateKey = new MemoryStream(new byte[] { });
     var AlicePublicKey = new MemoryStream(new byte[] { });

     // Create the Raw ECDH static keyring
     var staticConfiguration = new RawEcdhStaticConfigurations()
     {
      RawPrivateKeyToStaticPublicKey = new RawPrivateKeyToStaticPublicKeyInput
      {
       SenderStaticPrivateKey = BobPrivateKey,
       RecipientPublicKey = AlicePublicKey
      }
     };

     var createKeyringInput = new CreateRawEcdhKeyringInput()
     {
      CurveSpec = ECDHCurveSpec.ECC_NIST_P256,
      KeyAgreementScheme = staticConfiguration
     };

     var keyring = materialProviders.CreateRawEcdhKeyring(createKeyringInput);
```

Java

Contoh Java berikut menggunakan skema perjanjian `RawPrivateKeyToStaticPublicKey` kunci untuk secara statis mengkonfigurasi kunci pribadi pengirim dan kunci publik penerima. Kedua pasangan kunci berada di `ECC_NIST_P256` kurva.

```
private static void StaticRawKeyring() {
    // Instantiate material providers
    final MaterialProviders materialProviders =
      MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();

    KeyPair senderKeys = GetRawEccKey();
    KeyPair recipient = GetRawEccKey();

    // Create the Raw ECDH static keyring
    final CreateRawEcdhKeyringInput rawKeyringInput =
      CreateRawEcdhKeyringInput.builder()
        .curveSpec(ECDHCurveSpec.ECC_NIST_P256)
        .KeyAgreementScheme(
```

```
          RawEcdhStaticConfigurations.builder()
            .RawPrivateKeyToStaticPublicKey(
                RawPrivateKeyToStaticPublicKeyInput.builder()
                  // Must be a PEM-encoded private key

 .senderStaticPrivateKey(ByteBuffer.wrap(senderKeys.getPrivate().getEncoded()))
                  // Must be a DER-encoded X.509 public key

 .recipientPublicKey(ByteBuffer.wrap(recipient.getPublic().getEncoded()))
                  .build()
            )
            .build()
        ).build();

    final IKeyring staticKeyring =
 materialProviders.CreateRawEcdhKeyring(rawKeyringInput);
}
```

Python

Contoh Python berikut menggunakan skema perjanjian `RawEcdhStaticConfigurationsRawPrivateKeyToStaticPublicKey` kunci untuk secara statis mengkonfigurasi kunci pribadi pengirim dan kunci publik penerima. Kedua pasangan kunci berada di `ECC_NIST_P256` kurva.

```
import boto3
from aws_cryptographic_materialproviders.mpl.models import (
    CreateRawEcdhKeyringInput,
    RawEcdhStaticConfigurationsRawPrivateKeyToStaticPublicKey,
    RawPrivateKeyToStaticPublicKeyInput,
)
from aws_cryptography_primitives.smithygenerated.aws_cryptography_primitives.models
 import ECDHCurveSpec

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Must be a PEM-encoded private key
bob_private_key = get_private_key_bytes()
# Must be a DER-encoded X.509 public key
alice_public_key = get_public_key_bytes()
```

```
# Create the raw ECDH static keyring
raw_keyring_input = CreateRawEcdhKeyringInput(
    curve_spec = ECDHCurveSpec.ECC_NIST_P256,
    key_agreement_scheme =
 RawEcdhStaticConfigurationsRawPrivateKeyToStaticPublicKey(
        RawPrivateKeyToStaticPublicKeyInput(
            sender_static_private_key = bob_private_key,
            recipient_public_key = alice_public_key,
        )
    )
)

keyring = mat_prov.create_raw_ecdh_keyring(raw_keyring_input)
```

Rust

Contoh Python berikut menggunakan skema perjanjian `raw_ecdh_static_configuration` kunci untuk secara statis mengkonfigurasi kunci pribadi pengirim dan kunci publik penerima. Kedua pasangan kunci harus berada pada kurva yang sama.

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Optional: Create your encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Create keyring input
let raw_ecdh_static_configuration_input =
    RawPrivateKeyToStaticPublicKeyInput::builder()
        // Must be a UTF8 PEM-encoded private key
        .sender_static_private_key(private_key_sender_utf8_bytes)
        // Must be a UTF8 DER-encoded X.509 public key
        .recipient_public_key(public_key_recipient_utf8_bytes)
        .build()?;
```

```
let raw_ecdh_static_configuration =
 RawEcdhStaticConfigurations::RawPrivateKeyToStaticPublicKey(raw_ecdh_static_configuration_i

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create raw ECDH static keyring
let raw_ecdh_keyring = mpl
    .create_raw_ecdh_keyring()
    .curve_spec(ecdh_curve_spec)
    .key_agreement_scheme(raw_ecdh_static_configuration)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Optional: Create your encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
```

```
    "the data you are handling": "is what you think it is",
}

// Create keyring input
rawEcdhStaticConfigurationInput := mpltypes.RawPrivateKeyToStaticPublicKeyInput{
    SenderStaticPrivateKey: privateKeySender,
    RecipientPublicKey:     publicKeyRecipient,
}
rawECDHStaticConfiguration :=
 &mpltypes.RawEcdhStaticConfigurationsMemberRawPrivateKeyToStaticPublicKey{
    Value: rawEcdhStaticConfigurationInput,
}
rawEcdhKeyRingInput := mpltypes.CreateRawEcdhKeyringInput{
    CurveSpec:          ecdhCurveSpec,
    KeyAgreementScheme: rawECDHStaticConfiguration,
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create raw ECDH static keyring
rawEcdhKeyring, err := matProv.CreateRawEcdhKeyring(context.Background(),
 rawEcdhKeyRingInput)
if err != nil {
    panic(err)
}
```

EphemeralPrivateKeyToStaticPublicKey

Keyrings yang dikonfigurasi dengan skema perjanjian `EphemeralPrivateKeyToStaticPublicKey` kunci membuat key pair baru secara lokal dan mendapatkan kunci pembungkus bersama yang unik untuk setiap panggilan enkripsi.

Skema perjanjian kunci ini hanya dapat mengenkripsi pesan. Untuk mendekripsi pesan yang dienkripsi dengan skema perjanjian `EphemeralPrivateKeyToStaticPublicKey` kunci, Anda harus menggunakan skema perjanjian kunci penemuan yang dikonfigurasi dengan kunci publik penerima yang sama. Untuk mendekripsi, Anda dapat menggunakan keyring ECDH mentah dengan algoritma perjanjian `PublicKeyDiscovery`kunci, atau, jika kunci publik penerima berasal dari key

pair KMS perjanjian kunci asimetris, Anda dapat menggunakan keyring AWS KMS ECDH dengan skema perjanjian kunci. KmsPublicKeyDiscovery

Untuk menginisialisasi keyring ECDH mentah dengan skema perjanjian `EphemeralPrivateKeyToStaticPublicKey` kunci, berikan nilai-nilai berikut:

- Kunci publik penerima

  Anda harus memberikan kunci publik X.509 yang dikodekan DER penerima, juga dikenal sebagai `SubjectPublicKeyInfo` (SPKI), sebagaimana didefinisikan dalam RFC 5280.

  Anda dapat menentukan kunci publik dari perjanjian kunci asimetris KMS key pair atau kunci publik dari key pair yang dihasilkan di luar. AWS
- Spesifikasi kurva

  Mengidentifikasi spesifikasi kurva elips dalam kunci publik yang ditentukan.

  Pada enkripsi, keyring membuat key pair baru pada kurva yang ditentukan dan menggunakan kunci pribadi baru dan kunci publik tertentu untuk mendapatkan kunci pembungkus bersama.

  Nilai valid: `ECC_NIST_P256`, `ECC_NIS_P384`, `ECC_NIST_P512`

C# / .NET

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `EphemeralPrivateKeyToStaticPublicKey` kunci. Pada enkripsi, keyring akan membuat key pair baru secara lokal pada kurva yang ditentukan. `ECC_NIST_P256`

```
// Instantiate material providers
var materialProviders = new MaterialProviders(new MaterialProvidersConfig());
     var AlicePublicKey = new MemoryStream(new byte[] { });

     // Create the Raw ECDH ephemeral keyring
     var ephemeralConfiguration = new RawEcdhStaticConfigurations()
     {
      EphemeralPrivateKeyToStaticPublicKey = new
 EphemeralPrivateKeyToStaticPublicKeyInput
      {
       RecipientPublicKey = AlicePublicKey
      }
     };
```

```
     var createKeyringInput = new CreateRawEcdhKeyringInput()
     {
      CurveSpec = ECDHCurveSpec.ECC_NIST_P256,
      KeyAgreementScheme = ephemeralConfiguration
     };

     var keyring = materialProviders.CreateRawEcdhKeyring(createKeyringInput);
```

Java

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `EphemeralPrivateKeyToStaticPublicKey` kunci. Pada enkripsi, keyring akan membuat key pair baru secara lokal pada kurva yang ditentukan. `ECC_NIST_P256`

```
private static void EphemeralRawEcdhKeyring() {
    // Instantiate material providers
    final MaterialProviders materialProviders =
      MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();

    ByteBuffer recipientPublicKey = getPublicKeyBytes();

    // Create the Raw ECDH ephemeral keyring
    final CreateRawEcdhKeyringInput ephemeralInput =
      CreateRawEcdhKeyringInput.builder()
        .curveSpec(ECDHCurveSpec.ECC_NIST_P256)
        .KeyAgreementScheme(
          RawEcdhStaticConfigurations.builder()
            .EphemeralPrivateKeyToStaticPublicKey(
              EphemeralPrivateKeyToStaticPublicKeyInput.builder()
                .recipientPublicKey(recipientPublicKey)
                .build()
            )
            .build()
        ).build();

    final IKeyring ephemeralKeyring =
 materialProviders.CreateRawEcdhKeyring(ephemeralInput);
}
```

Python

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `RawEcdhStaticConfigurationsEphemeralPrivateKeyToStaticPublicKey` kunci. Pada enkripsi, keyring akan membuat key pair baru secara lokal pada kurva yang ditentukan. `ECC_NIST_P256`

```
import boto3
from aws_cryptographic_materialproviders.mpl.models import (
    CreateRawEcdhKeyringInput,
    RawEcdhStaticConfigurationsEphemeralPrivateKeyToStaticPublicKey,
    EphemeralPrivateKeyToStaticPublicKeyInput,
)
from aws_cryptography_primitives.smithygenerated.aws_cryptography_primitives.models
 import ECDHCurveSpec

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Your get_public_key_bytes must return a DER-encoded X.509 public key
recipient_public_key = get_public_key_bytes()

# Create the raw ECDH ephemeral private key keyring
ephemeral_input = CreateRawEcdhKeyringInput(
    curve_spec = ECDHCurveSpec.ECC_NIST_P256,
    key_agreement_scheme =
 RawEcdhStaticConfigurationsEphemeralPrivateKeyToStaticPublicKey(
        EphemeralPrivateKeyToStaticPublicKeyInput(
            recipient_public_key = recipient_public_key,
        )
    )
)

keyring = mat_prov.create_raw_ecdh_keyring(ephemeral_input)
```

Rust

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `ephemeral_raw_ecdh_static_configuration` kunci. Pada enkripsi, keyring akan membuat key pair baru secara lokal pada kurva yang ditentukan.

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Optional: Create your encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Load public key from UTF-8 encoded PEM files into a DER encoded public key.
let public_key_file_content =
 std::fs::read_to_string(Path::new(EXAMPLE_ECC_PUBLIC_KEY_FILENAME_RECIPIENT))?;
let parsed_public_key_file_content = parse(public_key_file_content)?;
let public_key_recipient_utf8_bytes = parsed_public_key_file_content.contents();

// Create EphemeralPrivateKeyToStaticPublicKeyInput
let ephemeral_raw_ecdh_static_configuration_input =
    EphemeralPrivateKeyToStaticPublicKeyInput::builder()
        // Must be a UTF8 DER-encoded X.509 public key
        .recipient_public_key(public_key_recipient_utf8_bytes)
        .build()?;

let ephemeral_raw_ecdh_static_configuration =

 RawEcdhStaticConfigurations::EphemeralPrivateKeyToStaticPublicKey(ephemeral_raw_ecdh_static

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create raw ECDH ephemeral private key keyring
let ephemeral_raw_ecdh_keyring = mpl
    .create_raw_ecdh_keyring()
    .curve_spec(ecdh_curve_spec)
    .key_agreement_scheme(ephemeral_raw_ecdh_static_configuration)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Optional: Create your encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Load public key from UTF-8 encoded PEM files into a DER encoded public key
publicKeyRecipient, err := LoadPublicKeyFromPEM(eccPublicKeyFileNameRecipient)
if err != nil {
    panic(err)
}

// Create EphemeralPrivateKeyToStaticPublicKeyInput
ephemeralRawEcdhStaticConfigurationInput :=
 mpltypes.EphemeralPrivateKeyToStaticPublicKeyInput{
    RecipientPublicKey: publicKeyRecipient,
}
ephemeralRawECDHStaticConfiguration :=
    mpltypes.RawEcdhStaticConfigurationsMemberEphemeralPrivateKeyToStaticPublicKey{
        Value: ephemeralRawEcdhStaticConfigurationInput,
```

```
    }

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create raw ECDH ephemeral private key keyring
rawEcdhKeyRingInput := mpltypes.CreateRawEcdhKeyringInput{
    CurveSpec:          ecdhCurveSpec,
    KeyAgreementScheme: &ephemeralRawECDHStaticConfiguration,
}
ecdhKeyring, err := matProv.CreateRawEcdhKeyring(context.Background(),
 rawEcdhKeyRingInput)
if err != nil {
    panic(err)
}
```

PublicKeyDiscovery

Saat mendekripsi, ini adalah praktik terbaik untuk menentukan kunci pembungkus yang dapat digunakan. AWS Encryption SDK Untuk mengikuti praktik terbaik ini, gunakan keyring ECDH yang menentukan kunci pribadi pengirim dan kunci publik penerima. Namun, Anda juga dapat membuat keyring penemuan ECDH mentah, yaitu keyring ECDH mentah yang dapat mendekripsi pesan apa pun di mana kunci publik kunci yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan. Skema perjanjian kunci ini hanya dapat mendekripsi pesan.

> **Important**
>
> Ketika Anda mendekripsi pesan menggunakan skema perjanjian `PublicKeyDiscovery` kunci, Anda menerima semua kunci publik, terlepas dari siapa yang memilikinya.

Untuk menginisialisasi keyring ECDH mentah dengan skema perjanjian `PublicKeyDiscovery` kunci, berikan nilai-nilai berikut:

- Kunci pribadi statis penerima

Anda harus memberikan kunci pribadi yang disandikan PEM penerima (PrivateKeyInfo struktur PKCS #8), seperti yang didefinisikan dalam RFC 5958.

- Spesifikasi kurva

  Mengidentifikasi spesifikasi kurva elips dalam kunci pribadi yang ditentukan. Pasangan kunci pengirim dan penerima harus memiliki spesifikasi kurva yang sama.

  Nilai valid: `ECC_NIST_P256`, `ECC_NIS_P384`, `ECC_NIST_P512`

C# / .NET

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `PublicKeyDiscovery` kunci. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari kunci pribadi yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
// Instantiate material providers
var materialProviders = new MaterialProviders(new MaterialProvidersConfig());
     var AlicePrivateKey = new MemoryStream(new byte[] { });

     // Create the Raw ECDH discovery keyring
     var discoveryConfiguration = new RawEcdhStaticConfigurations()
     {
      PublicKeyDiscovery = new PublicKeyDiscoveryInput
      {
       RecipientStaticPrivateKey = AlicePrivateKey
      }
     };

     var createKeyringInput = new CreateRawEcdhKeyringInput()
     {
      CurveSpec = ECDHCurveSpec.ECC_NIST_P256,
      KeyAgreementScheme = discoveryConfiguration
     };

     var keyring = materialProviders.CreateRawEcdhKeyring(createKeyringInput);
```

Java

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `PublicKeyDiscovery` kunci. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari kunci pribadi yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
private static void RawEcdhDiscovery() {
    // Instantiate material providers
    final MaterialProviders materialProviders =
      MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();

    KeyPair recipient = GetRawEccKey();

    // Create the Raw ECDH discovery keyring
    final CreateRawEcdhKeyringInput rawKeyringInput =
      CreateRawEcdhKeyringInput.builder()
        .curveSpec(ECDHCurveSpec.ECC_NIST_P256)
        .KeyAgreementScheme(
          RawEcdhStaticConfigurations.builder()
            .PublicKeyDiscovery(
              PublicKeyDiscoveryInput.builder()
                // Must be a PEM-encoded private key

 .recipientStaticPrivateKey(ByteBuffer.wrap(sender.getPrivate().getEncoded()))
                .build()
            )
            .build()
        ).build();

    final IKeyring publicKeyDiscovery  =
 materialProviders.CreateRawEcdhKeyring(rawKeyringInput);
}
```

Python

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `RawEcdhStaticConfigurationsPublicKeyDiscovery` kunci. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari kunci pribadi yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
import boto3
from aws_cryptographic_materialproviders.mpl.models import (
    CreateRawEcdhKeyringInput,
    RawEcdhStaticConfigurationsPublicKeyDiscovery,
    PublicKeyDiscoveryInput,
)
from aws_cryptography_primitives.smithygenerated.aws_cryptography_primitives.models
 import ECDHCurveSpec

# Instantiate the material providers library
mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

# Your get_private_key_bytes must return a PEM-encoded private key
recipient_private_key = get_private_key_bytes()

# Create the raw ECDH discovery keyring
raw_keyring_input = CreateRawEcdhKeyringInput(
    curve_spec = ECDHCurveSpec.ECC_NIST_P256,
    key_agreement_scheme = RawEcdhStaticConfigurationsPublicKeyDiscovery(
        PublicKeyDiscoveryInput(
            recipient_static_private_key = recipient_private_key,
        )
    )
)

keyring = mat_prov.create_raw_ecdh_keyring(raw_keyring_input)
```

Rust

Contoh berikut membuat keyring ECDH mentah dengan skema perjanjian `discovery_raw_ecdh_static_configuration` kunci. Keyring ini dapat mendekripsi pesan apa pun di mana kunci publik dari kunci pribadi yang ditentukan cocok dengan kunci publik penerima yang disimpan pada ciphertext pesan.

```
// Instantiate the AWS Encryption SDK client and material providers library
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;
```

```
// Optional: Create your encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Load keys from UTF-8 encoded PEM files.
let mut file = File::open(Path::new(EXAMPLE_ECC_PRIVATE_KEY_FILENAME_RECIPIENT))?;
let mut private_key_recipient_utf8_bytes = Vec::new();
file.read_to_end(&mut private_key_recipient_utf8_bytes)?;

// Create PublicKeyDiscoveryInput
let discovery_raw_ecdh_static_configuration_input =
    PublicKeyDiscoveryInput::builder()
        // Must be a UTF8 PEM-encoded private key
        .recipient_static_private_key(private_key_recipient_utf8_bytes)
        .build()?;

let discovery_raw_ecdh_static_configuration =

 RawEcdhStaticConfigurations::PublicKeyDiscovery(discovery_raw_ecdh_static_configuration_inp

// Create raw ECDH discovery private key keyring
let discovery_raw_ecdh_keyring = mpl
    .create_raw_ecdh_keyring()
    .curve_spec(ecdh_curve_spec)
    .key_agreement_scheme(discovery_raw_ecdh_static_configuration)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
```

```
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Optional: Create your encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Load keys from UTF-8 encoded PEM files.
privateKeyRecipient, err := os.ReadFile(eccPrivateKeyFileNameRecipient)
if err != nil {
    panic(err)
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create PublicKeyDiscoveryInput
discoveryRawEcdhStaticConfigurationInput := mpltypes.PublicKeyDiscoveryInput{
    RecipientStaticPrivateKey: privateKeyRecipient,
}

discoveryRawEcdhStaticConfiguration :=
 &mpltypes.RawEcdhStaticConfigurationsMemberPublicKeyDiscovery{
    Value: discoveryRawEcdhStaticConfigurationInput,
}
```

```
// Create raw ECDH discovery private key keyring
discoveryRawEcdhKeyringInput := mpltypes.CreateRawEcdhKeyringInput{
    CurveSpec:          ecdhCurveSpec,
    KeyAgreementScheme: discoveryRawEcdhStaticConfiguration,
}

discoveryRawEcdhKeyring, err := matProv.CreateRawEcdhKeyring(context.Background(),
 discoveryRawEcdhKeyringInput)
if err != nil {
    panic(err)
}
```

Multi-kunci

Anda dapat menggabungkan keyrings menjadi multi-keyring. Multi-keyring adalah keyring yang terdiri dari satu atau lebih gantungan kunci individu dari jenis yang sama atau berbeda. Efeknya seperti menggunakan beberapa gantungan kunci dalam satu seri. Bila Anda menggunakan multi-keyring untuk mengenkripsi data, salah satu kunci pembungkus di salah satu keyrings nya dapat mendekripsi data tersebut.

Saat Anda membuat multi-keyring untuk mengenkripsi data, Anda menunjuk salah satu keyring sebagai keyring generator. Semua gantungan kunci lainnya dikenal sebagai gantungan kunci anak. Generator keyring menghasilkan dan mengenkripsi kunci data plaintext. Kemudian, semua kunci pembungkus di semua keyring anak mengenkripsi kunci data teks biasa yang sama. Multi-keyring mengembalikan kunci plaintext dan satu kunci data terenkripsi untuk setiap kunci pembungkus di multi-keyring. Jika keyring generator adalah keyring KMS, kunci generator di AWS KMS keyring menghasilkan dan mengenkripsi kunci plaintext. Kemudian, semua tambahan AWS KMS keys di AWS KMS keyring, dan semua kunci pembungkus di semua keyring anak di multi-keyring, mengenkripsi kunci plaintext yang sama.

Jika Anda membuat multi-keyring tanpa keyring generator, Anda dapat menggunakannya sendiri untuk mendekripsi data, tetapi tidak untuk mengenkripsi. Atau, untuk menggunakan multi-keyring tanpa keyring genertor dalam operasi enkripsi, Anda dapat menentukannya sebagai keyring anak di multi-keyring lain. Multi-keyring tanpa keyring generator tidak dapat ditetapkan sebagai keyring generator di multi-keyring lain.

Saat mendekripsi, AWS Encryption SDK menggunakan keyrings untuk mencoba mendekripsi salah satu kunci data terenkripsi. Gantungan kunci dipanggil dalam urutan yang ditentukan dalam multi-keyring. Pemrosesan berhenti segera setelah kunci apa pun di keyring apa pun dapat mendekripsi kunci data terenkripsi.

Dimulai pada versi 1.7. x, ketika kunci data terenkripsi dienkripsi di bawah keyring AWS Key Management Service (AWS KMS) (atau penyedia kunci master), selalu AWS Encryption SDK meneruskan ARN kunci AWS KMS key ke parameter operasi Dekripsi. `KeyId`AWS KMS Ini adalah praktik AWS KMS terbaik yang memastikan bahwa Anda mendekripsi kunci data terenkripsi dengan kunci pembungkus yang ingin Anda gunakan.

Untuk melihat contoh kerja multi-keyring, lihat:

- C: multi_keyring.cpp
- C#/.NET: .cs MultiKeyringExample
- JavaScript Node.js: multi_keyring.ts
- JavaScript Browser: multi_keyring.ts
- Jawa: MultiKeyringExample.java
- Python: multi_keyring_example.py

Untuk membuat multi-keyring, pertama-tama buat instance keyrings anak. Dalam contoh ini, kami menggunakan AWS KMS keyring dan keyring Raw AES, tetapi Anda dapat menggabungkan keyrings yang didukung dalam multi-keyring.

C

```
/* Define an AWS KMS keyring. For details, see string.cpp */
struct aws_cryptosdk_keyring *kms_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder().Build(example_key);

// Define a Raw AES keyring. For details, see raw_aes_keyring.c */
struct aws_cryptosdk_keyring *aes_keyring = aws_cryptosdk_raw_aes_keyring_new(
        alloc, wrapping_key_namespace, wrapping_key_name, wrapping_key,
 AWS_CRYPTOSDK_AES256);
```

C# / .NET

```
// Define an AWS KMS keyring. For details, see AwsKmsKeyringExample.cs.
var kmsKeyring = materialProviders.CreateAwsKmsKeyring(createKmsKeyringInput);
```

```
// Define a Raw AES keyring. For details, see RawAESKeyringExample.cs.
var aesKeyring = materialProviders.CreateRawAesKeyring(createAesKeyringInput);
```

JavaScript Browser

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

```
import {
  KmsKeyringBrowser,
  KMS,
  getClient,
  RawAesKeyringWebCrypto,
  RawAesWrappingSuiteIdentifier,
  MultiKeyringWebCrypto,
  buildClient,
  CommitmentPolicy,
  synchronousRandomValues,
} from '@aws-crypto/client-browser'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

const clientProvider = getClient(KMS, { credentials })

// Define an AWS KMS keyring. For details, see kms_simple.ts.
const kmsKeyring = new KmsKeyringBrowser({ generatorKeyId: exampleKey })

// Define a Raw AES keyring. For details, see aes_simple.ts.
const aesKeyring = new RawAesKeyringWebCrypto({ keyName, keyNamespace,
 wrappingSuite, masterKey })
```

JavaScript Node.js

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

```
import {
  MultiKeyringNode,
  KmsKeyringNode,
  RawAesKeyringNode,
  RawAesWrappingSuiteIdentifier,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

// Define an AWS KMS keyring. For details, see kms_simple.ts.
const kmsKeyring = new KmsKeyringNode({ generatorKeyId: exampleKey })

// Define a Raw AES keyring. For details, see raw_aes_keyring_node.ts.
const aesKeyring = new RawAesKeyringNode({ keyName, keyNamespace, wrappingSuite,
 unencryptedMasterKey })
```

Java

```
// Define the raw AES keyring.
final MaterialProviders matProv = MaterialProviders.builder()
        .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
        .build();
final CreateRawAesKeyringInput createRawAesKeyringInput =
 CreateRawAesKeyringInput.builder()
        .keyName("AES_256_012")
        .keyNamespace("HSM_01")
        .wrappingKey(AESWrappingKey)
        .wrappingAlg(AesWrappingAlg.ALG_AES256_GCM_IV12_TAG16)
        .build();
IKeyring rawAesKeyring = matProv.CreateRawAesKeyring(createRawAesKeyringInput);

// Define the AWS KMS keyring.
final CreateAwsKmsMrkMultiKeyringInput createAwsKmsMrkMultiKeyringInput =
 CreateAwsKmsMrkMultiKeyringInput.builder()
        .generator(kmsKeyArn)
        .build();
IKeyring awsKmsMrkMultiKeyring =
 matProv.CreateAwsKmsMrkMultiKeyring(createAwsKmsMrkMultiKeyringInput);
```

Python

Contoh berikut membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. `REQUIRE_ENCRYPT_REQUIRE_DECRYPT`

```
# Create the AWS KMS keyring
kms_client = boto3.client('kms', region_name="us-west-2")

mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
    config=MaterialProvidersConfig()
)

kms_keyring_input: CreateAwsKmsKeyringInput = CreateAwsKmsKeyringInput(
    generator=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab,
    kms_client=kms_client
)

kms_keyring: IKeyring = mat_prov.create_aws_kms_keyring(
    input=kms_keyring_input
)

# Create Raw AES keyring
key_name_space = "HSM_01"
key_name = "AES_256_012"

raw_aes_keyring_input: CreateRawAesKeyringInput = CreateRawAesKeyringInput(
    key_namespace=key_name_space,
    key_name=key_name,
    wrapping_key=AESWrappingKey,
    wrapping_alg=AesWrappingAlg.ALG_AES256_GCM_IV12_TAG16
)

raw_aes_keyring: IKeyring = mat_prov.create_raw_aes_keyring(
    input=raw_aes_keyring_input
)
```

Rust

```
// Instantiate the AWS Encryption SDK client
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;
```

```
// Create the AWS KMS client
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create an AWS KMS keyring
let kms_keyring = mpl
    .create_aws_kms_keyring()
    .kms_key_id(kms_key_id)
    .kms_client(kms_client)
    .send()
    .await?;

// Create a Raw AES keyring
let key_namespace: &str = "my-key-namespace";
let key_name: &str = "my-aes-key-name";

let raw_aes_keyring = mpl
    .create_raw_aes_keyring()
    .key_name(key_name)
    .key_namespace(key_namespace)
    .wrapping_key(aws_smithy_types::Blob::new(AESWrappingKey))
    .wrapping_alg(AesWrappingAlg::AlgAes256GcmIv12Tag16)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
```

```
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
encryptionClient, err := client.NewClient(esdktypes.AwsEncryptionSdkConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}

// Create an AWS KMS keyring
awsKmsKeyringInput := mpltypes.CreateAwsKmsKeyringInput{
    KmsClient: kmsClient,
    KmsKeyId:  kmsKeyId,
}
awsKmsKeyring, err := matProv.CreateAwsKmsKeyring(context.Background(),
 awsKmsKeyringInput)
if err != nil {
    panic(err)
}

// Create a Raw AES keyring
var keyNamespace = "my-key-namespace"
var keyName = "my-aes-key-name"

aesKeyRingInput := mpltypes.CreateRawAesKeyringInput{
    KeyName:      keyName,
    KeyNamespace: keyNamespace,
    WrappingKey:  AESWrappingKey,
```

```
    WrappingAlg:  mpltypes.AesWrappingAlgAlgAes256GcmIv12Tag16,
}
aesKeyring, err := matProv.CreateRawAesKeyring(context.Background(),
 aesKeyRingInput)
```

Selanjutnya, buat multi-keyring dan tentukan keyring generatornya, jika ada. Dalam contoh ini, kami membuat multi-keyring di mana keyring adalah AWS KMS keyring generator dan keyring AES adalah keyring anak.

C

Dalam konstruktor multi-keyring di C, Anda hanya menentukan keyring generatornya.

```
struct aws_cryptosdk_keyring *multi_keyring = aws_cryptosdk_multi_keyring_new(alloc,
 kms_keyring);
```

Untuk menambahkan keyring anak ke multi-keyring Anda, gunakan metode ini. `aws_cryptosdk_multi_keyring_add_child` Anda perlu memanggil metode satu kali untuk setiap keyring anak yang Anda tambahkan.

```
// Add the Raw AES keyring (C only)
aws_cryptosdk_multi_keyring_add_child(multi_keyring, aes_keyring);
```

C# / .NET

`CreateMultiKeyringInput`Konstruktor.NET memungkinkan Anda menentukan keyring generator dan keyrings anak. `CreateMultiKeyringInput`Objek yang dihasilkan tidak dapat diubah.

```
var createMultiKeyringInput = new CreateMultiKeyringInput
{
    Generator = kmsKeyring,
    ChildKeyrings = new List<IKeyring>() {aesKeyring}
};

var multiKeyring = materialProviders.CreateMultiKeyring(createMultiKeyringInput);
```

JavaScript Browser

JavaScript multi-keyrings tidak dapat diubah. Konstruktor JavaScript multi-keyring memungkinkan Anda menentukan keyring generator dan beberapa keyring anak.

```
const clientProvider = getClient(KMS, { credentials })

const multiKeyring = new MultiKeyringWebCrypto(generator: kmsKeyring, children:
 [aesKeyring]);
```

JavaScript Node.js

JavaScript multi-keyrings tidak dapat diubah. Konstruktor JavaScript multi-keyring memungkinkan Anda menentukan keyring generator dan beberapa keyring anak.

```
const multiKeyring = new MultiKeyringNode(generator: kmsKeyring, children:
 [aesKeyring]);
```

Java

`CreateMultiKeyringInput`Konstruktor Java memungkinkan Anda menentukan keyring generator dan keyrings anak. `createMultiKeyringInput`Objek yang dihasilkan tidak dapat diubah.

```
final CreateMultiKeyringInput createMultiKeyringInput =
 CreateMultiKeyringInput.builder()
        .generator(awsKmsMrkMultiKeyring)
        .childKeyrings(Collections.singletonList(rawAesKeyring))
        .build();
IKeyring multiKeyring = matProv.CreateMultiKeyring(createMultiKeyringInput);
```

Python

```
multi_keyring_input: CreateMultiKeyringInput = CreateMultiKeyringInput(
    generator=kms_keyring,
    child_keyrings=[raw_aes_keyring]
)

multi_keyring: IKeyring = mat_prov.create_multi_keyring(
    input=multi_keyring_input
)
```

Rust

```
let multi_keyring = mpl
    .create_multi_keyring()
    .generator(kms_keyring.clone())
    .child_keyrings(vec![raw_aes_keyring.clone()])
    .send()
    .await?;
```

Go

```
createMultiKeyringInput := mpltypes.CreateMultiKeyringInput{
  Generator:     awsKmsKeyring,
  ChildKeyrings: []mpltypes.IKeyring{rawAESKeyring},
 }
 multiKeyring, err := matProv.CreateMultiKeyring(context.Background(),
 createMultiKeyringInput)
 if err != nil {
  panic(err)
 }
```

Sekarang, Anda dapat menggunakan multi-keyring untuk mengenkripsi dan mendekripsi data.

AWS Encryption SDK bahasa pemrograman

AWS Encryption SDK Ini tersedia untuk bahasa pemrograman berikut. Semua implementasi bahasa dapat dioperasikan secara interoperable. Anda dapat mengenkripsi dengan satu implementasi bahasa dan mendekripsi dengan yang lain. Interoperabilitas mungkin tunduk pada kendala bahasa. Jika demikian, kendala ini dijelaskan dalam topik tentang implementasi bahasa. Selain itu, saat mengenkripsi dan mendekripsi, Anda harus menggunakan keyring yang kompatibel, atau kunci master dan penyedia kunci master. Lihat perinciannya di the section called “Kompatibilitas keyring”.

Topik

AWS Encryption SDK for C

AWS Encryption SDK for C Ini menyediakan pustaka enkripsi sisi klien untuk pengembang yang menulis aplikasi di C. Ini juga berfungsi sebagai dasar untuk implementasi AWS Encryption SDK dalam bahasa pemrograman tingkat tinggi.

Seperti semua implementasi AWS Encryption SDK, AWS Encryption SDK for C menawarkan fitur perlindungan data tingkat lanjut. Ini termasuk enkripsi amplop, data otentikasi tambahan (AAD), dan rangkaian algoritma kunci simetris yang aman, diautentikasi, seperti AES-GCM 256-bit dengan derivasi dan penandatanganan kunci.

Semua implementasi khusus bahasa sepenuhnya dapat AWS Encryption SDK dioperasikan. Misalnya, Anda dapat mengenkripsi data dengan AWS Encryption SDK for C dan mendekripsi dengan implementasi bahasa yang didukung, termasuk CLI Enkripsi AWS .

AWS Encryption SDK for C Membutuhkan AWS SDK untuk C++ untuk berinteraksi dengan AWS Key Management Service (AWS KMS). Anda perlu menggunakannya hanya jika Anda menggunakan

AWS KMS keyring opsional. Namun, AWS Encryption SDK tidak memerlukan AWS KMS atau AWS layanan lainnya.

Pelajari Lebih Lanjut

- Untuk detail tentang pemrograman dengan AWS Encryption SDK for C, lihat contoh C, contoh di aws-encryption-sdk-c repositori aktif GitHub, dan dokumentasi AWS Encryption SDK for C API.
- Untuk diskusi tentang cara menggunakan data AWS Encryption SDK for C untuk mengenkripsi sehingga Anda dapat mendekripsi dalam beberapa Wilayah AWS, lihat Cara mendekripsi ciphertext di beberapa wilayah dengan di C di Blog Keamanan. AWS Encryption SDK AWS

Topik

Instalasi AWS Encryption SDK for C

Instal versi terbaru dari file AWS Encryption SDK for C.

> **Note**
>
> Semua versi yang AWS Encryption SDK for C lebih awal dari 2.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.0. x dan yang lebih baru ke versi terbaru AWS Encryption SDK for C tanpa kode atau perubahan data apa pun. Namun, fitur keamanan baru diperkenalkan di versi 2.0. x tidak kompatibel ke belakang. Untuk memperbarui dari versi lebih awal dari 1.7. x ke versi 2.0. x dan yang lebih baru, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi AWS Encryption SDK for C. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

Anda dapat menemukan petunjuk terperinci untuk menginstal dan membangun file README dari aws-encryption-sdk-crepositori. AWS Encryption SDK for C Ini termasuk instruksi untuk membangun di Amazon Linux, Ubuntu, macOS, dan platform Windows.

Sebelum Anda mulai, putuskan apakah Anda ingin menggunakan AWS KMS gantungan kunci di. AWS Encryption SDK Jika Anda menggunakan AWS KMS keyring, Anda perlu menginstal. AWS SDK untuk C++ AWS SDK diperlukan untuk berinteraksi dengan AWS Key Management Service(AWS KMS). Ketika Anda menggunakan AWS KMS keyrings, AWS Encryption SDK digunakan AWS KMS untuk menghasilkan dan melindungi kunci enkripsi yang melindungi data Anda.

Anda tidak perlu menginstal AWS SDK untuk C++ jika Anda menggunakan jenis keyring lain, seperti keyring AES mentah, keyring RSA mentah, atau multi-keyring yang tidak menyertakan keyring. AWS KMS Namun, saat menggunakan tipe keyring mentah, Anda perlu membuat dan melindungi kunci pembungkus mentah Anda sendiri.

Jika Anda mengalami masalah dengan instalasi Anda, ajukan masalah di `aws-encryption-sdk-c` repositori atau gunakan tautan umpan balik apa pun di halaman ini.

Menggunakan AWS Encryption SDK for C

Topik ini menjelaskan beberapa fitur yang tidak didukung dalam implementasi bahasa pemrograman lainnya. AWS Encryption SDK for C

Contoh di bagian ini menunjukkan cara menggunakan versi 2.0. x dan yang lebih baru AWS Encryption SDK for C. Untuk contoh yang menggunakan versi sebelumnya, temukan rilis Anda di daftar Rilis dari aws-encryption-sdk-c repositori repositori di. GitHub

Untuk detail tentang pemrograman dengan AWS Encryption SDK for C, lihat contoh C, contoh di aws-encryption-sdk-c repositori aktif GitHub, dan dokumentasi AWS Encryption SDK for C API.

Lihat juga: Gantungan kunci

Topik

- Pola untuk mengenkripsi dan mendekripsi data
- Penghitungan referensi

Pola untuk mengenkripsi dan mendekripsi data

Bila Anda menggunakan AWS Encryption SDK for C, Anda mengikuti pola yang mirip dengan ini: membuat keyring, membuat CMM yang menggunakan keyring, membuat sesi yang menggunakan CMM (dan keyring), dan kemudian memproses sesi.

1. Memuat string kesalahan.

   Panggil `aws_cryptosdk_load_error_strings()` metode dalam kode C atau C ++ Anda. Ini memuat informasi kesalahan yang sangat berguna untuk debugging.

   Anda hanya perlu memanggilnya sekali, seperti dalam `main` metode Anda.

   ```
   /* Load error strings for debugging */
   aws_cryptosdk_load_error_strings();
   ```

2. Buat keyring.

   Konfigurasikan keyring Anda dengan tombol pembungkus yang ingin Anda gunakan untuk mengenkripsi kunci data Anda. Contoh ini menggunakan AWS KMS keyring dengan satu AWS KMS key, tetapi Anda dapat menggunakan semua jenis keyring sebagai gantinya.

   Untuk mengidentifikasi AWS KMS key dalam keyring enkripsi di AWS Encryption SDK for C, tentukan kunci ARN atau alias ARN. Dalam keyring dekripsi, Anda harus menggunakan kunci ARN. Lihat perinciannya di Mengidentifikasi AWS KMS keys dalam AWS KMS keyring.

   ```
   const char * KEY_ARN = "arn:aws:kms:us-
   west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
   struct aws_cryptosdk_keyring *kms_keyring =
          Aws::Cryptosdk::KmsKeyring::Builder().Build(KEY_ARN);
   ```

3. Buat sesi.

   Dalam AWS Encryption SDK for C, Anda menggunakan sesi untuk mengenkripsi pesan teks biasa tunggal atau mendekripsi pesan ciphertext tunggal, terlepas dari ukurannya. Sesi mempertahankan status pesan selama pemrosesannya.

   Konfigurasikan sesi Anda dengan pengalokasi, keyring, dan mode: atau. `AWS_CRYPTOSDK_ENCRYPT` `AWS_CRYPTOSDK_DECRYPT` Jika Anda perlu mengubah mode sesi, gunakan `aws_cryptosdk_session_reset` metode ini.

   Saat Anda membuat sesi dengan keyring, AWS Encryption SDK for C secara otomatis membuat manajer materi kriptografi default (CMM) untuk Anda. Anda tidak perlu membuat, memelihara, atau menghancurkan objek ini.

   Misalnya, sesi berikut menggunakan pengalokasi dan keyring yang didefinisikan pada langkah 1. Saat Anda mengenkripsi data, modenya adalah`AWS_CRYPTOSDK_ENCRYPT`.

```
struct aws_cryptosdk_session * session =
 aws_cryptosdk_session_new_from_keyring_2(allocator, AWS_CRYPTOSDK_ENCRYPT,
 kms_keyring);
```

4. Enkripsi atau dekripsi data.

   Untuk memproses data dalam sesi, gunakan `aws_cryptosdk_session_process` metode ini. Jika buffer input cukup besar untuk menampung seluruh plaintext, dan buffer output cukup besar untuk menampung seluruh ciphertext, Anda dapat menelepon. `aws_cryptosdk_session_process_full` Namun, jika Anda perlu menangani data streaming, Anda dapat menelepon `aws_cryptosdk_session_process` dalam satu lingkaran. Sebagai contoh, lihat contoh file_streaming.cpp. `aws_cryptosdk_session_process_full`Ini diperkenalkan dalam AWS Encryption SDK versi 1.9. x dan 2.2. x.

   Ketika sesi dikonfigurasi untuk mengenkripsi data, bidang plaintext menjelaskan input dan bidang ciphertext menggambarkan output. `plaintext`Bidang menyimpan pesan yang ingin Anda enkripsi dan `ciphertext` bidang mendapatkan pesan terenkripsi yang dikembalikan oleh metode enkripsi.

```
/* Encrypting data */
aws_cryptosdk_session_process_full(session,
                                   ciphertext,
                                   ciphertext_buffer_size,
                                   &ciphertext_length,
                                   plaintext,
                                   plaintext_length)
```

   Ketika sesi dikonfigurasi untuk mendekripsi data, bidang ciphertext menjelaskan input dan bidang plaintext menggambarkan output. `ciphertext`Bidang menyimpan pesan terenkripsi yang dikembalikan oleh metode enkripsi, dan `plaintext` bidang mendapatkan pesan teks biasa yang dikembalikan oleh metode dekripsi.

   Untuk mendekripsi data, panggil metode. `aws_cryptosdk_session_process_full`

```
/* Decrypting data */
aws_cryptosdk_session_process_full(session,
                                   plaintext,
                                   plaintext_buffer_size,
```

```
                                    &plaintext_length,
                                    ciphertext,
                                    ciphertext_length)
```

Penghitungan referensi

Untuk mencegah kebocoran memori, pastikan untuk melepaskan referensi Anda ke semua objek yang Anda buat saat Anda selesai menggunakannya. Jika tidak, Anda akan berakhir dengan kebocoran memori. SDK menyediakan metode untuk mempermudah tugas ini.

Setiap kali Anda membuat objek induk dengan salah satu objek anak berikut, objek induk mendapatkan dan mempertahankan referensi ke objek anak, sebagai berikut:

- Sebuah keyring, seperti membuat sesi dengan keyring
- Manajer materi kriptografi default (CMM), seperti membuat sesi atau CMM khusus dengan CMM default
- Cache kunci data, seperti membuat CMM caching dengan keyring dan cache

Kecuali Anda memerlukan referensi independen ke objek anak, Anda dapat melepaskan referensi Anda ke objek anak segera setelah Anda membuat objek induk. Referensi yang tersisa untuk objek anak dilepaskan ketika objek induk dihancurkan. Pola ini memastikan bahwa Anda mempertahankan referensi ke setiap objek hanya selama Anda membutuhkannya, dan Anda tidak membocorkan memori karena referensi yang belum dirilis.

Anda hanya bertanggung jawab untuk merilis referensi ke objek anak yang Anda buat secara eksplisit. Anda tidak bertanggung jawab untuk mengelola referensi ke objek apa pun yang dibuat SDK untuk Anda. Jika SDK membuat objek, seperti CMM default yang ditambahkan `aws_cryptosdk_caching_cmm_new_from_keyring` metode ke sesi, SDK mengelola pembuatan dan penghancuran objek dan referensinya.

Dalam contoh berikut, ketika Anda membuat sesi dengan keyring, sesi mendapatkan referensi ke keyring, dan mempertahankan referensi itu sampai sesi dihancurkan. Jika Anda tidak perlu mempertahankan referensi tambahan ke keyring, Anda dapat menggunakan `aws_cryptosdk_keyring_release` metode untuk melepaskan objek keyring segera setelah sesi dibuat. Metode ini mengurangi jumlah referensi untuk keyring. Referensi sesi ke keyring dilepaskan saat Anda menelepon `aws_cryptosdk_session_destroy` untuk menghancurkan sesi.

```
// The session gets a reference to the keyring.
struct aws_cryptosdk_session *session =
 aws_cryptosdk_session_new_from_keyring_2(alloc, AWS_CRYPTOSDK_ENCRYPT, keyring);

// After you create a session with a keyring, release the reference to the keyring
 object.
aws_cryptosdk_keyring_release(keyring);
```

Untuk tugas yang lebih kompleks, seperti menggunakan kembali keyring untuk beberapa sesi atau menentukan rangkaian algoritme dalam CMM, Anda mungkin perlu mempertahankan referensi independen ke objek. Jika demikian, jangan segera panggil metode rilis. Sebagai gantinya, lepaskan referensi Anda saat Anda tidak lagi menggunakan objek, selain menghancurkan sesi.

Teknik penghitungan referensi ini juga berfungsi ketika Anda menggunakan alternatif CMMs, seperti CMM caching untuk caching kunci data. Saat Anda membuat CMM caching dari cache dan keyring, CMM caching mendapatkan referensi ke kedua objek. Kecuali Anda membutuhkannya untuk tugas lain, Anda dapat melepaskan referensi independen Anda ke cache dan keyring segera setelah CMM caching dibuat. Kemudian, ketika Anda membuat sesi dengan CMM caching, Anda dapat melepaskan referensi Anda ke CMM caching.

Perhatikan bahwa Anda hanya bertanggung jawab untuk merilis referensi ke objek yang Anda buat secara eksplisit. Objek yang dibuat metode untuk Anda, seperti CMM default yang mendasari CMM caching, dikelola oleh metode.

```
/ Create the caching CMM from a cache and a keyring.
struct aws_cryptosdk_cmm *caching_cmm =
 aws_cryptosdk_caching_cmm_new_from_keyring(allocator, cache, kms_keyring, NULL, 60,
 AWS_TIMESTAMP_SECS);

// Release your references to the cache and the keyring.
aws_cryptosdk_materials_cache_release(cache);
aws_cryptosdk_keyring_release(kms_keyring);

// Create a session with the caching CMM.
struct aws_cryptosdk_session *session = aws_cryptosdk_session_new_from_cmm_2(allocator,
 AWS_CRYPTOSDK_ENCRYPT, caching_cmm);

// Release your references to the caching CMM.
aws_cryptosdk_cmm_release(caching_cmm);

// ...
```

```
aws_cryptosdk_session_destroy(session);
```

AWS Encryption SDK for C contoh

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK for C mendekripsi data.

Contoh di bagian ini menunjukkan cara menggunakan versi 2.0. x dan kemudian AWS Encryption SDK for C. Untuk contoh yang menggunakan versi sebelumnya, temukan rilis Anda di daftar Rilis dari aws-encryption-sdk-c repositori repositori di. GitHub

Ketika Anda menginstal dan membangun AWS Encryption SDK for C, kode sumber untuk ini dan contoh lainnya disertakan dalam `examples` subdirektori, dan mereka dikompilasi dan dibangun ke dalam `build` direktori. Anda juga dapat menemukannya di contoh subdirektori aws-encryption-sdk-crepositori di. GitHub

Topik

- Mengenkripsi dan mendekripsi string

Mengenkripsi dan mendekripsi string

Contoh berikut menunjukkan kepada Anda bagaimana menggunakan AWS Encryption SDK for C untuk mengenkripsi dan mendekripsi string.

Contoh ini menampilkan AWS KMS keyring, jenis keyring yang menggunakan AWS KMS key in AWS Key Management Service (AWS KMS) untuk menghasilkan dan mengenkripsi kunci data. Contohnya termasuk kode yang ditulis dalam C ++. Yang AWS Encryption SDK for C mengharuskan AWS SDK untuk C++ untuk memanggil AWS KMS saat menggunakan AWS KMS keyrings. Jika Anda menggunakan keyring yang tidak berinteraksi AWS KMS, seperti keyring AES mentah, keyring RSA mentah, atau multi-keyring yang tidak menyertakan keyring, tidak diperlukan. AWS KMS AWS SDK untuk C++

Untuk bantuan membuat AWS KMS key, lihat Membuat Kunci di Panduan AWS Key Management Service Pengembang. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Lihat contoh kode lengkap: string.cpp

Topik

Enkripsi string

Bagian pertama dari contoh ini menggunakan AWS KMS keyring dengan satu AWS KMS key untuk mengenkripsi string plaintext.

Langkah 1. Memuat string kesalahan.

Panggil `aws_cryptosdk_load_error_strings()` metode dalam kode C atau C ++ Anda. Ini memuat informasi kesalahan yang sangat berguna untuk debugging.

Anda hanya perlu memanggilnya sekali, seperti dalam `main` metode Anda.

```
/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();
```

Langkah 2: Bangun keyring.

Buat AWS KMS keyring untuk enkripsi. Keyring dalam contoh ini dikonfigurasi dengan satu AWS KMS key, tetapi Anda dapat mengonfigurasi AWS KMS keyring dengan beberapa AWS KMS keys, termasuk AWS KMS keys di akun yang berbeda Wilayah AWS dan berbeda.

Untuk mengidentifikasi AWS KMS key dalam keyring enkripsi di AWS Encryption SDK for C, tentukan kunci ARN atau alias ARN. Dalam keyring dekripsi, Anda harus menggunakan kunci ARN. Lihat perinciannya di Mengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Mengidentifikasi AWS KMS keys dalam AWS KMS keyring

Ketika Anda membuat keyring dengan beberapa AWS KMS keys, Anda menentukan yang AWS KMS key digunakan untuk menghasilkan dan mengenkripsi kunci data plaintext, dan array opsional tambahan yang mengenkripsi kunci data plaintext AWS KMS keys yang sama. Dalam hal ini, Anda hanya menentukan generator AWS KMS key.

Sebelum menjalankan kode ini, ganti contoh kunci ARN dengan yang valid.

```
const char * key_arn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
struct aws_cryptosdk_keyring *kms_keyring =
       Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn);
```

Langkah 3: Buat sesi.

Buat sesi menggunakan pengalokasi, enumerator mode, dan keyring.

Setiap sesi membutuhkan mode: baik `AWS_CRYPTOSDK_ENCRYPT` untuk mengenkripsi atau `AWS_CRYPTOSDK_DECRYPT` mendekripsi. Untuk mengubah mode sesi yang ada, gunakan `aws_cryptosdk_session_reset` metode ini.

Setelah membuat sesi dengan keyring, Anda dapat melepaskan referensi ke keyring menggunakan metode yang disediakan SDK. Sesi mempertahankan referensi ke objek keyring selama masa pakainya. Referensi ke keyring dan objek sesi dilepaskan saat Anda menghancurkan sesi. Teknik penghitungan referensi ini membantu mencegah kebocoran memori dan mencegah objek dilepaskan saat sedang digunakan.

```
struct aws_cryptosdk_session *session =
       aws_cryptosdk_session_new_from_keyring_2(alloc, AWS_CRYPTOSDK_ENCRYPT,
 kms_keyring);

/* When you add the keyring to the session, release the keyring object */
aws_cryptosdk_keyring_release(kms_keyring);
```

Langkah 4: Atur konteks enkripsi.

Konteks enkripsi adalah data otentikasi tambahan yang sewenang-wenang dan tidak rahasia. Ketika Anda menyediakan konteks enkripsi pada enkripsi, AWS Encryption SDK kriptografis mengikat konteks enkripsi ke ciphertext sehingga konteks enkripsi yang sama diperlukan untuk mendekripsi data. Menggunakan konteks enkripsi adalah opsional, tetapi kami merekomendasikannya sebagai praktik terbaik.

Pertama, buat tabel hash yang menyertakan string konteks enkripsi.

```
/* Allocate a hash table for the encryption context */
int set_up_enc_ctx(struct aws_allocator *alloc, struct aws_hash_table *my_enc_ctx)

// Create encryption context strings
AWS_STATIC_STRING_FROM_LITERAL(enc_ctx_key1, "Example");
AWS_STATIC_STRING_FROM_LITERAL(enc_ctx_value1, "String");
```

```
AWS_STATIC_STRING_FROM_LITERAL(enc_ctx_key2, "Company");
AWS_STATIC_STRING_FROM_LITERAL(enc_ctx_value2, "MyCryptoCorp");

// Put the key-value pairs in the hash table
aws_hash_table_put(my_enc_ctx, enc_ctx_key1, (void *)enc_ctx_value1, &was_created)
aws_hash_table_put(my_enc_ctx, enc_ctx_key2, (void *)enc_ctx_value2, &was_created)
```

Dapatkan pointer yang bisa berubah ke konteks enkripsi dalam sesi. Kemudian, gunakan `aws_cryptosdk_enc_ctx_clone` fungsi untuk menyalin konteks enkripsi ke dalam sesi. Simpan salinan `my_enc_ctx` sehingga Anda dapat memvalidasi nilai setelah mendekripsi data.

Konteks enkripsi adalah bagian dari sesi, bukan parameter yang diteruskan ke fungsi proses sesi. Ini menjamin bahwa konteks enkripsi yang sama digunakan untuk setiap segmen pesan, bahkan jika fungsi proses sesi dipanggil beberapa kali untuk mengenkripsi seluruh pesan.

```
struct aws_hash_table *session_enc_ctx =
 aws_cryptosdk_session_get_enc_ctx_ptr_mut(session);

aws_cryptosdk_enc_ctx_clone(alloc, session_enc_ctx, my_enc_ctx)
```

Langkah 5: Enkripsi string.

Untuk mengenkripsi string plaintext, gunakan `aws_cryptosdk_session_process_full` metode dengan sesi dalam mode enkripsi. Metode ini, diperkenalkan dalam AWS Encryption SDK versi 1.9. x dan 2.2. x, dirancang untuk enkripsi dan dekripsi non-streaming. Untuk menangani streaming data, panggil `aws_cryptosdk_session_process` dalam satu lingkaran.

Saat mengenkripsi, bidang plaintext adalah bidang input; bidang ciphertext adalah bidang keluaran. Saat pemrosesan selesai, `ciphertext_output` bidang berisi pesan terenkripsi, termasuk ciphertext aktual, kunci data terenkripsi, dan konteks enkripsi. Anda dapat mendekripsi pesan terenkripsi ini dengan menggunakan AWS Encryption SDK untuk setiap bahasa pemrograman yang didukung.

```
/* Gets the length of the plaintext that the session processed */
size_t ciphertext_len_output;
if (AWS_OP_SUCCESS != aws_cryptosdk_session_process_full(session,
                                    ciphertext_output,
                                    ciphertext_buf_sz_output,
                                    &ciphertext_len_output,
                                    plaintext_input,
```

```
                                    plaintext_len_input)) {
    aws_cryptosdk_session_destroy(session);
    return 8;
}
```

Langkah 6: Bersihkan sesi.

Langkah terakhir menghancurkan sesi termasuk referensi ke CMM dan keyring.

Jika Anda lebih suka, alih-alih menghancurkan sesi, Anda dapat menggunakan kembali sesi dengan keyring dan CMM yang sama untuk mendekripsi string, atau untuk mengenkripsi atau mendekripsi pesan lain. Untuk menggunakan sesi untuk mendekripsi, gunakan `aws_cryptosdk_session_reset` metode untuk mengubah mode ke. `AWS_CRYPTOSDK_DECRYPT`

Dekripsi string

Bagian kedua dari contoh ini mendekripsi pesan terenkripsi yang berisi ciphertext dari string asli.

Langkah 1: Muat string kesalahan.

Panggil `aws_cryptosdk_load_error_strings()` metode dalam kode C atau C ++ Anda. Ini memuat informasi kesalahan yang sangat berguna untuk debugging.

Anda hanya perlu memanggilnya sekali, seperti dalam `main` metode Anda.

```
/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();
```

Langkah 2: Bangun keyring.

Saat Anda mendekripsi data AWS KMS, Anda meneruskan pesan terenkripsi yang dikembalikan oleh API enkripsi. Decrypt API tidak mengambil AWS KMS key sebagai input. Sebaliknya, AWS KMS menggunakan yang sama AWS KMS key untuk mendekripsi ciphertext yang digunakan untuk mengenkripsi itu. Namun, AWS Encryption SDK memungkinkan Anda menentukan AWS KMS keyring dengan enkripsi dan AWS KMS keys dekripsi.

Saat mendekripsi, Anda dapat mengonfigurasi keyring hanya dengan AWS KMS keys yang ingin Anda gunakan untuk mendekripsi pesan terenkripsi. Misalnya, Anda mungkin ingin membuat keyring hanya dengan AWS KMS key yang digunakan oleh peran tertentu dalam organisasi Anda.

Tidak AWS Encryption SDK akan pernah menggunakan AWS KMS key kecuali muncul di keyring dekripsi. Jika SDK tidak dapat mendekripsi kunci data terenkripsi dengan menggunakan keyring AWS KMS keys dalam yang Anda berikan, baik karena tidak ada AWS KMS keys dalam keyring yang digunakan untuk mengenkripsi salah satu kunci data, atau karena pemanggil tidak memiliki izin untuk menggunakan AWS KMS keys dalam keyring untuk mendekripsi, panggilan dekripsi gagal.

Ketika Anda menentukan AWS KMS key untuk keyring dekripsi, Anda harus menggunakan kunci ARN. Alias hanya ARNs diizinkan dalam gantungan kunci enkripsi. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihatMengidentifikasi AWS KMS keys dalam AWS KMS keyring.

Dalam contoh ini, kami menentukan keyring yang dikonfigurasi dengan yang sama AWS KMS key digunakan untuk mengenkripsi string. Sebelum menjalankan kode ini, ganti contoh kunci ARN dengan yang valid.

```
const char * key_arn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"

struct aws_cryptosdk_keyring *kms_keyring =
        Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn);
```

Langkah 3: Buat sesi.

Buat sesi menggunakan pengalokasi dan keyring. Untuk mengkonfigurasi sesi untuk dekripsi, konfigurasikan sesi dengan mode. `AWS_CRYPTOSDK_DECRYPT`

Setelah membuat sesi dengan keyring, Anda dapat melepaskan referensi ke keyring menggunakan metode yang disediakan SDK. Sesi mempertahankan referensi ke objek keyring selama masa pakainya, dan sesi dan keyring dilepaskan saat Anda menghancurkan sesi. Teknik penghitungan referensi ini membantu mencegah kebocoran memori dan mencegah objek dilepaskan saat sedang digunakan.

```
struct aws_cryptosdk_session *session =
 aws_cryptosdk_session_new_from_keyring_2(alloc, AWS_CRYPTOSDK_DECRYPT,
 kms_keyring);

/* When you add the keyring to the session, release the keyring object */
aws_cryptosdk_keyring_release(kms_keyring);
```

Langkah 4: Dekripsi string.

Untuk mendekripsi string, gunakan `aws_cryptosdk_session_process_full` metode dengan sesi yang dikonfigurasi untuk dekripsi. Metode ini, diperkenalkan dalam AWS Encryption SDK versi 1.9. x dan 2.2. x, dirancang untuk enkripsi dan dekripsi non-streaming. Untuk menangani streaming data, panggil `aws_cryptosdk_session_process` dalam satu lingkaran.

Saat mendekripsi, bidang ciphertext adalah bidang input dan bidang plaintext adalah bidang keluaran. `ciphertext_input`Bidang menyimpan pesan terenkripsi yang dikembalikan oleh metode enkripsi. Saat pemrosesan selesai, `plaintext_output` bidang berisi string plaintext (didekripsi).

```
size_t plaintext_len_output;

if (AWS_OP_SUCCESS != aws_cryptosdk_session_process_full(session,
                                  plaintext_output,
                                  plaintext_buf_sz_output,
                                  &plaintext_len_output,
                                  ciphertext_input,
                                  ciphertext_len_input)) {
    aws_cryptosdk_session_destroy(session);
    return 13;
}
```

Langkah 5: Verifikasi konteks enkripsi.

Pastikan bahwa konteks enkripsi yang sebenarnya — yang digunakan untuk mendekripsi pesan — berisi konteks enkripsi yang Anda berikan saat mengenkripsi pesan. Konteks enkripsi yang sebenarnya mungkin mencakup pasangan tambahan, karena pengelola materi kriptografi (CMM) dapat menambahkan pasangan ke konteks enkripsi yang disediakan sebelum mengenkripsi pesan.

Di dalam AWS Encryption SDK for C, Anda tidak diharuskan untuk menyediakan konteks enkripsi saat mendekripsi karena konteks enkripsi disertakan dalam pesan terenkripsi yang dikembalikan SDK. Namun, sebelum mengembalikan pesan teks biasa, fungsi dekripsi Anda harus memverifikasi bahwa semua pasangan dalam konteks enkripsi yang disediakan muncul dalam konteks enkripsi yang digunakan untuk mendekripsi pesan.

Pertama, dapatkan pointer read-only ke tabel hash di sesi. Tabel hash ini berisi konteks enkripsi yang digunakan untuk mendekripsi pesan.

```
const struct aws_hash_table *session_enc_ctx =
 aws_cryptosdk_session_get_enc_ctx_ptr(session);
```

Kemudian, loop melalui konteks enkripsi dalam tabel `my_enc_ctx` hash yang Anda salin saat mengenkripsi. Verifikasi bahwa setiap pasangan dalam tabel `my_enc_ctx` hash yang digunakan untuk mengenkripsi muncul di tabel `session_enc_ctx` hash yang digunakan untuk mendekripsi. Jika ada kunci yang hilang, atau kunci itu memiliki nilai yang berbeda, hentikan pemrosesan dan tulis pesan kesalahan.

```
for (struct aws_hash_iter iter = aws_hash_iter_begin(my_enc_ctx); !
aws_hash_iter_done(&iter);
      aws_hash_iter_next(&iter)) {
     struct aws_hash_element *session_enc_ctx_kv_pair;
     aws_hash_table_find(session_enc_ctx, iter.element.key,
 &session_enc_ctx_kv_pair)

    if (!session_enc_ctx_kv_pair ||
        !aws_string_eq(
            (struct aws_string *)iter.element.value, (struct aws_string
 *)session_enc_ctx_kv_pair->value)) {
        fprintf(stderr, "Wrong encryption context!\n");
        abort();
    }
}
```

Langkah 6: Bersihkan sesi.

Setelah Anda memverifikasi konteks enkripsi, Anda dapat menghancurkan sesi, atau menggunakannya kembali. Jika Anda perlu mengkonfigurasi ulang sesi, gunakan `aws_cryptosdk_session_reset` metode ini.

```
aws_cryptosdk_session_destroy(session);
```

AWS Encryption SDK untuk .NET

The AWS Encryption SDK for .NET adalah pustaka enkripsi sisi klien untuk pengembang yang menulis aplikasi dalam C # dan bahasa pemrograman.NET lainnya. Hal ini didukung di Windows, macOS, dan Linux.

> **Note**
>
> Versi 4.0.0 AWS Encryption SDK untuk .NET menyimpang dari Spesifikasi Pesan. AWS Encryption SDK Akibatnya, pesan yang dienkripsi oleh versi 4.0.0 hanya dapat didekripsi oleh versi 4.0.0 atau yang lebih baru untuk .NET. AWS Encryption SDK Mereka tidak dapat didekripsi oleh implementasi bahasa pemrograman lainnya.
> Versi 4.0.1 AWS Encryption SDK untuk .NET menulis pesan sesuai dengan Spesifikasi AWS Encryption SDK Pesan, dan interoperable dengan implementasi bahasa pemrograman lainnya. Secara default, versi 4.0.1 dapat membaca pesan yang dienkripsi oleh versi 4.0.0. Namun, jika Anda tidak ingin mendekripsi pesan yang dienkripsi oleh versi 4.0.0, Anda dapat menentukan `NetV4_0_0_RetryPolicy`properti untuk mencegah klien membaca pesan-pesan ini. Untuk informasi lebih lanjut, lihat catatan rilis v4.0.1 di aws-encryption-sdk repositori di. GitHub

AWS Encryption SDK Untuk .NET berbeda dari beberapa implementasi bahasa pemrograman lainnya dengan AWS Encryption SDK cara berikut:

- Tidak ada dukungan untuk caching kunci data

  > **Note**
  >
  > Versi 4. x dari AWS Encryption SDK untuk .NET mendukung keyring AWS KMS Hierarchical, solusi caching bahan kriptografi alternatif.

- Tidak ada dukungan untuk streaming data
- Tidak ada pencatatan atau jejak tumpukan dari AWS Encryption SDK untuk .NET
- Membutuhkan AWS SDK for .NET

The AWS Encryption SDK for .NET mencakup semua fitur keamanan yang diperkenalkan dalam versi 2.0. x dan yang lebih baru dari implementasi bahasa lain dari. AWS Encryption SDK Namun, jika Anda menggunakan AWS Encryption SDK untuk.NET untuk mendekripsi data yang dienkripsi oleh pra-2.0. x versi implementasi bahasa lain dari AWS Encryption SDK, Anda mungkin perlu menyesuaikan kebijakan komitmen Anda. Lihat perinciannya di Cara menetapkan kebijakan komitmen Anda.

The AWS Encryption SDK for .NET adalah produk dari AWS Encryption SDK in Dafny, bahasa verifikasi formal di mana Anda menulis spesifikasi, kode untuk mengimplementasikannya, dan bukti untuk mengujinya. Hasilnya adalah perpustakaan yang mengimplementasikan fitur-fitur AWS Encryption SDK dalam kerangka kerja yang menjamin kebenaran fungsional.

Pelajari Lebih Lanjut

- Untuk contoh yang menunjukkan cara mengonfigurasi opsi di AWS Encryption SDK, seperti menentukan rangkaian algoritme alternatif, membatasi kunci data terenkripsi, dan menggunakan kunci AWS KMS Multi-region, lihat. Mengkonfigurasi AWS Encryption SDK
- Untuk detail tentang pemrograman dengan AWS Encryption SDK for .NET, lihat `aws-encryption-sdk-net`direktori aws-encryption-sdk repositori di. GitHub

Topik

- Instalasi AWS Encryption SDK untuk .NET
- Debugging AWS Encryption SDK untuk .NET
- AWS Encryption SDK untuk contoh.NET

Instalasi AWS Encryption SDK untuk .NET

The AWS Encryption SDK for .NET tersedia sebagai `AWS.Cryptography.EncryptionSDK`paket di NuGet. Untuk detail tentang menginstal dan membangun AWS Encryption SDK untuk .NET, lihat file README.md di repositori. `aws-encryption-sdk-net`

Versi 3.x

> Versi 3. x dari AWS Encryption SDK untuk .NET mendukung .NET Framework 4.5.2 - 4.8 hanya pada Windows. Ini mendukung .NET Core 3.0+ dan .NET 5.0 dan kemudian pada semua sistem operasi yang didukung.

Versi 4.x

> Versi 4. x dari AWS Encryption SDK untuk .NET mendukung .NET 6.0 dan .NET Framework net48 dan yang lebih baru. Versi 4. x membutuhkan AWS SDK untuk.NET v3.

AWS Encryption SDK Untuk .NET membutuhkan SDK for .NET bahkan jika Anda tidak menggunakan kunci AWS Key Management Service (AWS KMS). Itu diinstal dengan NuGet paket. Namun, kecuali

Anda menggunakan AWS KMS kunci, AWS Encryption SDK untuk .NET tidak memerlukan Akun AWS, AWS kredensi, atau interaksi dengan layanan apa pun AWS . Untuk bantuan menyiapkan AWS akun jika Anda membutuhkannya, lihatMenggunakan AWS Encryption SDK dengan AWS KMS.

Debugging AWS Encryption SDK untuk .NET

The AWS Encryption SDK for .NET tidak menghasilkan log apa pun. Pengecualian di AWS Encryption SDK for .NET menghasilkan pesan pengecualian, tetapi tidak ada jejak tumpukan.

Untuk membantu Anda men-debug, pastikan untuk mengaktifkan login. SDK for .NET Log dan pesan kesalahan dari SDK for .NET dapat membantu Anda membedakan kesalahan yang timbul SDK for .NET dari yang ada di AWS Encryption SDK untuk .NET. Untuk bantuan terkait SDK for .NET logging, lihat AWSLoggingdi Panduan AWS SDK for .NET Pengembang. (Untuk melihat topiknya, perluas bagian konten Open to view .NET Framework.)

AWS Encryption SDK untuk contoh.NET

Contoh berikut menunjukkan pola pengkodean dasar yang Anda gunakan saat pemrograman dengan AWS Encryption SDK for .NET. Secara khusus, Anda membuat instance perpustakaan AWS Encryption SDK dan penyedia materi. Kemudian, sebelum memanggil setiap metode, Anda membuat instance objek yang mendefinisikan input untuk metode tersebut. Ini sangat mirip dengan pola pengkodean yang Anda gunakan di SDK for .NET.

Untuk contoh yang menunjukkan cara mengonfigurasi opsi di AWS Encryption SDK, seperti menentukan rangkaian algoritme alternatif, membatasi kunci data terenkripsi, dan menggunakan kunci AWS KMS Multi-region, lihat. Mengkonfigurasi AWS Encryption SDK

Untuk lebih banyak contoh pemrograman dengan AWS Encryption SDK untuk .NET, lihat contoh di `aws-encryption-sdk-net` direktori `aws-encryption-sdk` repositori pada. GitHub

Mengenkripsi data di untuk .NET AWS Encryption SDK

Contoh ini menunjukkan pola dasar untuk mengenkripsi data. Ini mengenkripsi file kecil dengan kunci data yang dilindungi oleh satu kunci AWS KMS pembungkus.

Langkah 1: Buat instance AWS Encryption SDK dan perpustakaan penyedia materi.

Mulailah dengan membuat instance perpustakaan penyedia AWS Encryption SDK dan materi. Anda akan menggunakan metode dalam AWS Encryption SDK untuk mengenkripsi dan

mendekripsi data. Anda akan menggunakan metode di pustaka penyedia materi untuk membuat keyrings yang menentukan kunci mana yang melindungi data Anda.

Cara Anda membuat instance AWS Encryption SDK dan pustaka penyedia materi berbeda antara versi 3. x dan 4. x dari AWS Encryption SDK untuk .NET. Semua langkah berikut adalah sama untuk kedua versi 3. x dan 4. x dari AWS Encryption SDK untuk .NET.

Version 3.x

```
// Instantiate the AWS Encryption SDK and material providers
var encryptionSdk = AwsEncryptionSdkFactory.CreateDefaultAwsEncryptionSdk();
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders(
```

Version 4.x

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());
```

Langkah 2: Buat objek input untuk keyring.

Setiap metode yang membuat keyring memiliki kelas objek input yang sesuai. Misalnya, untuk membuat objek masukan untuk `CreateAwsKmsKeyring()` metode, buat instance `CreateAwsKmsKeyringInput` kelas.

Meskipun input untuk keyring ini tidak menentukan kunci generator, kunci KMS tunggal yang ditentukan oleh `KmsKeyId` parameter adalah kunci generator. Ini menghasilkan dan mengenkripsi kunci data yang mengenkripsi data.

Objek masukan ini membutuhkan AWS KMS klien untuk kunci KMS. Wilayah AWS Untuk membuat AWS KMS klien, buat instance `AmazonKeyManagementServiceClient` kelas di. SDK for .NET Memanggil `AmazonKeyManagementServiceClient()` konstruktor tanpa parameter membuat klien dengan nilai default.

Dalam AWS KMS keyring yang digunakan untuk mengenkripsi dengan AWS Encryption SDK for .NET, Anda dapat mengidentifikasi kunci KMS dengan menggunakan ID kunci, kunci ARN, nama alias, atau alias ARN. Dalam AWS KMS keyring yang digunakan untuk mendekripsi, Anda harus menggunakan ARN kunci untuk mengidentifikasi setiap kunci KMS. Jika Anda berencana

untuk menggunakan kembali keyring enkripsi Anda untuk mendekripsi, gunakan pengenal ARN kunci untuk semua kunci KMS.

```
string keyArn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Instantiate the keyring input object
var kmsKeyringInput = new CreateAwsKmsKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = keyArn
};
```

Langkah 3: Buat keyring.

Untuk membuat keyring, panggil metode keyring dengan objek input keyring. Contoh ini menggunakan `CreateAwsKmsKeyring()` metode, yang hanya membutuhkan satu kunci KMS.

```
var keyring = materialProviders.CreateAwsKmsKeyring(kmsKeyringInput);
```

Langkah 4: Tentukan konteks enkripsi.

Konteks enkripsi adalah elemen opsional, tetapi sangat direkomendasikan dari operasi kriptografi dalam. AWS Encryption SDK Anda dapat menentukan satu atau lebih pasangan nilai kunci non-rahasia.

> **Note**
>
> Dengan versi 4. x dari AWS Encryption SDK untuk .NET, Anda dapat memerlukan konteks enkripsi di semua permintaan enkripsi dengan konteks enkripsi CMM yang diperlukan.

```
// Define the encryption context
var encryptionContext = new Dictionary<string, string>()
{
    {"purpose", "test"}
};
```

Langkah 5: Buat objek input untuk mengenkripsi.

Sebelum memanggil `Encrypt()` metode, buat instance dari `EncryptInput` kelas.

```
string plaintext = File.ReadAllText("C:\\Documents\\CryptoTest\\TestFile.txt");

// Define the encrypt input
var encryptInput = new EncryptInput
{
    Plaintext = plaintext,
    Keyring = keyring,
    EncryptionContext = encryptionContext
};
```

Langkah 6: Enkripsi plaintext.

Gunakan `Encrypt()` metode AWS Encryption SDK untuk mengenkripsi plaintext menggunakan keyring yang Anda tentukan.

`Encrypt()` Metode `EncryptOutput` yang dikembalikan memiliki metode untuk mendapatkan pesan terenkripsi (`Ciphertext`), konteks enkripsi, dan rangkaian algoritma.

```
var encryptOutput = encryptionSdk.Encrypt(encryptInput);
```

Langkah 7: Dapatkan pesan terenkripsi.

`Decrypt()`Metode dalam AWS Encryption SDK for .NET mengambil `Ciphertext` anggota `EncryptOutput` instance.

`Ciphertext`Anggota `EncryptOutput` objek adalah pesan terenkripsi, objek portabel yang mencakup data terenkripsi, kunci data terenkripsi, dan metadata, termasuk konteks enkripsi. Anda dapat menyimpan pesan terenkripsi dengan aman untuk waktu yang lama atau mengirimkannya ke `Decrypt()` metode untuk memulihkan teks biasa.

```
var encryptedMessage = encryptOutput.Ciphertext;
```

Mendekripsi dalam mode ketat di untuk.NET AWS Encryption SDK

Praktik terbaik menyarankan Anda menentukan kunci yang Anda gunakan untuk mendekripsi data, opsi yang dikenal sebagai mode ketat. Hanya AWS Encryption SDK menggunakan kunci KMS yang

Anda tentukan dalam keyring Anda untuk mendekripsi ciphertext. Kunci dalam keyring dekripsi Anda harus menyertakan setidaknya salah satu kunci yang mengenkripsi data.

Contoh ini menunjukkan pola dasar dekripsi dalam mode ketat dengan AWS Encryption SDK untuk .NET.

Langkah 1: Buat instance perpustakaan penyedia materi AWS Encryption SDK dan.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());
```

Langkah 2: Buat objek input untuk keyring Anda.

Untuk menentukan parameter untuk metode keyring, buat objek input. Setiap metode keyring di AWS Encryption SDK for .NET memiliki objek input yang sesuai. Karena contoh ini menggunakan `CreateAwsKmsKeyring()` metode untuk membuat keyring, itu membuat instance `CreateAwsKmsKeyringInput` kelas untuk input.

Dalam keyring dekripsi, Anda harus menggunakan ARN kunci untuk mengidentifikasi kunci KMS.

```
string keyArn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Instantiate the keyring input object
var kmsKeyringInput = new CreateAwsKmsKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = keyArn
};
```

Langkah 3: Buat keyring.

Untuk membuat keyring dekripsi, contoh ini menggunakan `CreateAwsKmsKeyring()` metode dan objek input keyring.

```
var keyring = materialProviders.CreateAwsKmsKeyring(kmsKeyringInput);
```

Langkah 4: Buat objek input untuk mendekripsi.

Untuk membuat objek masukan untuk `Decrypt()` metode ini, buat instance kelas. `DecryptInput`

`Ciphertext`Parameter `DecryptInput()` konstruktor mengambil `Ciphertext` anggota `EncryptOutput` objek yang dikembalikan `Encrypt()` metode. `Ciphertext`Properti mewakili pesan terenkripsi, yang mencakup data terenkripsi, kunci data terenkripsi, dan metadata yang diperlukan untuk mendekripsi pesan. AWS Encryption SDK

Dengan versi 4. x dari AWS Encryption SDK untuk .NET, Anda dapat menggunakan `EncryptionContext` parameter opsional untuk menentukan konteks enkripsi Anda dalam `Decrypt()` metode.

Gunakan `EncryptionContext` parameter untuk memverifikasi bahwa konteks enkripsi yang digunakan pada enkripsi disertakan dalam konteks enkripsi yang digunakan untuk mendekripsi ciphertext. AWS Encryption SDK Menambahkan pasangan ke konteks enkripsi, termasuk tanda tangan digital jika Anda menggunakan rangkaian algoritme dengan penandatanganan, seperti rangkaian algoritme default.

```
var encryptedMessage = encryptOutput.Ciphertext;

var decryptInput = new DecryptInput
{
    Ciphertext = encryptedMessage,
    Keyring = keyring,
    EncryptionContext = encryptionContext // OPTIONAL
};
```

Langkah 5: Dekripsi ciphertext.

```
var decryptOutput = encryptionSdk.Decrypt(decryptInput);
```

Langkah 6: Verifikasi konteks enkripsi - Versi 3. x

`Decrypt()`Metode versi 3. x dari AWS Encryption SDK untuk .NET tidak mengambil konteks enkripsi. Ini mendapatkan nilai konteks enkripsi dari metadata dalam pesan terenkripsi. Namun, sebelum mengembalikan atau menggunakan plaintext, ini adalah praktik terbaik untuk memverifikasi bahwa konteks enkripsi yang digunakan untuk mendekripsi ciphertext mencakup konteks enkripsi yang Anda berikan saat mengenkripsi.

Verifikasi bahwa konteks enkripsi yang digunakan pada enkripsi disertakan dalam konteks enkripsi yang digunakan untuk mendekripsi ciphertext. AWS Encryption SDK Menambahkan pasangan ke konteks enkripsi, termasuk tanda tangan digital jika Anda menggunakan rangkaian algoritme dengan penandatanganan, seperti rangkaian algoritme default.

```
// Verify the encryption context
string contextKey = "purpose";
string contextValue = "test";

if (!decryptOutput.EncryptionContext.TryGetValue(contextKey, out var
 decryptContextValue)
    || !decryptContextValue.Equals(contextValue))
{
    throw new Exception("Encryption context does not match expected values");
}
```

Mendekripsi dengan keyring penemuan di for .NET AWS Encryption SDK

Daripada menentukan kunci KMS untuk dekripsi, Anda dapat memberikan keyring AWS KMS penemuan, yang merupakan keyring yang tidak menentukan kunci KMS apa pun. Keyring penemuan memungkinkan AWS Encryption SDK dekripsi data dengan menggunakan kunci KMS mana pun yang dienkripsi, asalkan penelepon memiliki izin dekripsi pada kunci tersebut. Untuk praktik terbaik, tambahkan filter penemuan yang membatasi kunci KMS yang dapat digunakan untuk kunci khusus Akun AWS partisi tertentu.

The AWS Encryption SDK for .NET menyediakan keyring penemuan dasar yang membutuhkan AWS KMS klien dan penemuan multi-keyring yang mengharuskan Anda menentukan satu atau lebih. Wilayah AWS Klien dan Wilayah membatasi kunci KMS yang dapat digunakan untuk mendekripsi pesan terenkripsi. Objek input untuk kedua keyring mengambil filter penemuan yang direkomendasikan.

Contoh berikut menunjukkan pola untuk mendekripsi data dengan keyring AWS KMS penemuan dan filter penemuan.

Langkah 1: Buat instance AWS Encryption SDK dan perpustakaan penyedia materi.

```
// Instantiate the AWS Encryption SDK and material providers
var esdk =  new ESDK(new AwsEncryptionSdkConfig());
var mpl = new MaterialProviders(new MaterialProvidersConfig());
```

Langkah 2: Buat objek input untuk keyring.

Untuk menentukan parameter untuk metode keyring, buat objek input. Setiap metode keyring di AWS Encryption SDK for .NET memiliki objek input yang sesuai. Karena contoh ini menggunakan

`CreateAwsKmsDiscoveryKeyring()` metode untuk membuat keyring, itu membuat instance `CreateAwsKmsDiscoveryKeyringInput` kelas untuk input.

```
List<string> accounts = new List<string> { "111122223333" };

var discoveryKeyringInput = new CreateAwsKmsDiscoveryKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    DiscoveryFilter = new DiscoveryFilter()
    {
        AccountIds = accounts,
        Partition = "aws"
    }
};
```

Langkah 3: Buat keyring.

Untuk membuat keyring dekripsi, contoh ini menggunakan `CreateAwsKmsDiscoveryKeyring()` metode dan objek input keyring.

```
var discoveryKeyring =
 materialProviders.CreateAwsKmsDiscoveryKeyring(discoveryKeyringInput);
```

Langkah 4: Buat objek input untuk mendekripsi.

Untuk membuat objek masukan untuk `Decrypt()` metode ini, buat instance kelas. `DecryptInput` Nilai `Ciphertext` parameter adalah `Ciphertext` anggota `EncryptOutput` objek yang dikembalikan `Encrypt()` metode.

Dengan versi 4. x dari AWS Encryption SDK untuk .NET, Anda dapat menggunakan `EncryptionContext` parameter opsional untuk menentukan konteks enkripsi Anda dalam `Decrypt()` metode.

Gunakan `EncryptionContext` parameter untuk memverifikasi bahwa konteks enkripsi yang digunakan pada enkripsi disertakan dalam konteks enkripsi yang digunakan untuk mendekripsi ciphertext. AWS Encryption SDK Menambahkan pasangan ke konteks enkripsi, termasuk tanda tangan digital jika Anda menggunakan rangkaian algoritme dengan penandatanganan, seperti rangkaian algoritme default.

```
var ciphertext = encryptOutput.Ciphertext;
```

```
var decryptInput = new DecryptInput
{
    Ciphertext = ciphertext,
    Keyring = discoveryKeyring,
    EncryptionContext = encryptionContext // OPTIONAL

};
var decryptOutput = encryptionSdk.Decrypt(decryptInput);
```

Langkah 5: Verifikasi konteks enkripsi - Versi 3. x

`Decrypt()`Metode versi 3. x dari AWS Encryption SDK untuk .NET tidak mengambil konteks enkripsi pada`Decrypt()`. Ini mendapatkan nilai konteks enkripsi dari metadata dalam pesan terenkripsi. Namun, sebelum mengembalikan atau menggunakan plaintext, ini adalah praktik terbaik untuk memverifikasi bahwa konteks enkripsi yang digunakan untuk mendekripsi ciphertext mencakup konteks enkripsi yang Anda berikan saat mengenkripsi.

Verifikasi bahwa konteks enkripsi yang digunakan pada enkripsi disertakan dalam konteks enkripsi yang digunakan untuk mendekripsi ciphertext. AWS Encryption SDK Menambahkan pasangan ke konteks enkripsi, termasuk tanda tangan digital jika Anda menggunakan rangkaian algoritme dengan penandatanganan, seperti rangkaian algoritme default.

```
// Verify the encryption context
string contextKey = "purpose";
string contextValue = "test";

if (!decryptOutput.EncryptionContext.TryGetValue(contextKey, out var
 decryptContextValue)
    || !decryptContextValue.Equals(contextValue))
{
    throw new Exception("Encryption context does not match expected values");
}
```

AWS Encryption SDK untuk Go

Topik ini menjelaskan cara menginstal dan menggunakan AWS Encryption SDK for Go. Untuk detail tentang pemrograman dengan AWS Encryption SDK for Go, lihat direktori go dari aws-encryption-sdk repositori di. GitHub

The AWS Encryption SDK for Go berbeda dari beberapa implementasi bahasa pemrograman lainnya dengan AWS Encryption SDK cara berikut:

- Tidak ada dukungan untuk caching kunci data. Namun, AWS Encryption SDK for Go mendukung keyring AWS KMS Hierarchical, solusi caching bahan kriptografi alternatif.
- Tidak ada dukungan untuk streaming data

The AWS Encryption SDK for Go mencakup semua fitur keamanan yang diperkenalkan di versi 2.0.x dan yang lebih baru dari implementasi bahasa lain dari. AWS Encryption SDK Namun, jika Anda menggunakan AWS Encryption SDK for Go untuk mendekripsi data yang dienkripsi oleh pra-2.0.x versi implementasi bahasa lain dari AWS Encryption SDK, Anda mungkin perlu menyesuaikan kebijakan komitmen Anda. Lihat perinciannya di Cara menetapkan kebijakan komitmen Anda.

The AWS Encryption SDK for Go adalah produk dari AWS Encryption SDK in Dafny, bahasa verifikasi formal di mana Anda menulis spesifikasi, kode untuk mengimplementasikannya, dan bukti untuk mengujinya. Hasilnya adalah perpustakaan yang mengimplementasikan fitur-fitur AWS Encryption SDK dalam kerangka kerja yang menjamin kebenaran fungsional.

Pelajari Lebih Lanjut

- Untuk contoh yang menunjukkan cara mengonfigurasi opsi di AWS Encryption SDK, seperti menentukan rangkaian algoritme alternatif, membatasi kunci data terenkripsi, dan menggunakan kunci AWS KMS Multi-region, lihat. Mengkonfigurasi AWS Encryption SDK
- Untuk contoh yang menunjukkan cara mengonfigurasi dan menggunakan AWS Encryption SDK for Go, lihat contoh Go di aws-encryption-sdk repositori aktif. GitHub

Topik

Prasyarat

Sebelum Anda menginstal AWS Encryption SDK for Go, pastikan Anda memiliki prasyarat berikut.

Versi Go yang didukung

Go 1.23 atau yang lebih baru diperlukan oleh AWS Encryption SDK for Go.

Untuk informasi selengkapnya tentang mengunduh dan menginstal Go, lihat Instalasi Go.

Penginstalan

Instal versi terbaru AWS Encryption SDK untuk Go. Untuk detail tentang menginstal dan membangun AWS Encryption SDK untuk Go, lihat README.md di direktori go repositori di aws-encryption-sdk. GitHub

Pasang versi terbaru

- Instal AWS Encryption SDK untuk Go

```
go get github.com/aws/aws-encryption-sdk/releases/go/encryption-sdk@latest
```

- Instal Perpustakaan Penyedia Materi Kriptografi (MPL)

```
go get github.com/aws/aws-cryptographic-material-providers-library/releases/go/mpl
```

AWS Encryption SDK for Java

Topik ini menjelaskan cara menginstal dan menggunakan AWS Encryption SDK for Java. Untuk detail tentang pemrograman dengan AWS Encryption SDK for Java, lihat aws-encryption-sdk-javarepositori di. GitHub Untuk dokumentasi API, lihat Javadoc untuk dokumen. AWS Encryption SDK for Java

Topik

- Prasyarat
- Penginstalan
- AWS Encryption SDK for Java contoh

Prasyarat

Sebelum Anda menginstal AWS Encryption SDK for Java, pastikan Anda memiliki prasyarat berikut.

Lingkungan pengembangan Java

Anda akan membutuhkan Java 8 atau yang lebih baru. Di situs web Oracle, buka Unduhan Java SE, kemudian unduh dan instal Java SE Development Kit (JDK).

Jika Anda menggunakan Oracle JDK, Anda juga harus mengunduh dan menginstal File Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy.

Kastil Goyang

AWS Encryption SDK for Java Membutuhkan Kastil Bouncy.

- AWS Encryption SDK for Java versi 1.6.1 dan yang lebih baru menggunakan Bouncy Castle untuk membuat serial dan deserialisasi objek kriptografi. Anda dapat menggunakan Bouncy Castle atau Bouncy Castle FIPS untuk memenuhi persyaratan ini. Untuk bantuan menginstal dan mengonfigurasi FIPS Bouncy Castle, lihat Dokumentasi BC FIPS, terutama Panduan Pengguna dan Kebijakan Keamanan. PDFs
- Versi sebelumnya AWS Encryption SDK for Java menggunakan API kriptografi Bouncy Castle untuk Java. Persyaratan ini hanya dipenuhi oleh Kastil Bouncy non-FIPS.

Jika Anda tidak memiliki Bouncy Castle, buka Unduh Bouncy Castle for Java untuk mengunduh file penyedia yang sesuai dengan JDK Anda. Anda juga dapat menggunakan Apache Maven untuk mendapatkan artefak untuk penyedia Bouncy Castle standar (bcprov-ext-jdk15on) atau artefak untuk Bouncy Castle FIPS (bc-fips).

AWS SDK for Java

Versi 3. x dari AWS Encryption SDK for Java membutuhkan AWS SDK for Java 2.x, bahkan jika Anda tidak menggunakan AWS KMS gantungan kunci.

Versi 2. x atau sebelumnya AWS Encryption SDK for Java tidak memerlukan AWS SDK for Java. Namun, AWS SDK for Java diperlukan untuk menggunakan AWS Key Management Service(AWS KMS) sebagai penyedia kunci utama. Dimulai pada AWS Encryption SDK for Java versi 2.4.0, AWS Encryption SDK for Java mendukung versi 1.x dan 2.x dari versi. AWS SDK for Java AWS Encryption SDK kode untuk AWS SDK for Java 1.x dan 2.x dapat dioperasikan. Misalnya, Anda dapat mengenkripsi data dengan AWS Encryption SDK kode yang mendukung AWS SDK for Java 1.x dan mendekripsi menggunakan kode yang mendukung AWS SDK for Java 2.x (atau sebaliknya). Versi yang AWS Encryption SDK for Java lebih awal dari 2.4.0 hanya mendukung AWS SDK for Java 1.x. Untuk informasi tentang memperbarui versi Anda AWS Encryption SDK, lihatMigrasi Anda AWS Encryption SDK.

Saat memperbarui AWS Encryption SDK for Java kode Anda dari AWS SDK for Java 1.x ke AWS SDK for Java 2.x, ganti referensi ke `AWSKMSantarmuka` di AWS SDK for Java 1.x dengan referensi ke `KmsClientantarmuka` di. AWS SDK for Java 2.x AWS Encryption SDK for Java Tidak mendukung `KmsAsyncClientantarmuka`. Juga, perbarui kode Anda untuk menggunakan objek AWS KMS-related di `kmssdkv2` namespace, bukan namespace. `kms`

Untuk menginstal AWS SDK for Java, gunakan Apache Maven.

- Untuk mengimpor keseluruhan AWS SDK for Java sebagai dependensi, deklarasikan dalam file Anda. `pom.xml`
- Untuk membuat dependensi hanya untuk AWS KMS modul di AWS SDK for Java 1.x, ikuti instruksi untuk menentukan modul tertentu, dan atur ke. `artifactId` `aws-java-sdk-kms`
- Untuk membuat dependensi hanya untuk AWS KMS modul di AWS SDK for Java 2.x, ikuti instruksi untuk menentukan modul tertentu. Atur `groupId` ke `software.amazon.awssdk` dan `artifactId` kekms.

Untuk perubahan lainnya, lihat Apa yang berbeda antara AWS SDK for Java 1.x dan 2.x di Panduan AWS SDK for Java 2.x Pengembang.

Contoh Java dalam Panduan AWS Encryption SDK Pengembang menggunakan file AWS SDK for Java 2.x.

Penginstalan

Instal versi terbaru dari file AWS Encryption SDK for Java.

> **Note**
>
> Semua versi yang AWS Encryption SDK for Java lebih awal dari 2.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.0. x dan yang lebih baru ke versi terbaru AWS Encryption SDK for Java tanpa kode atau perubahan data. Namun, fitur keamanan baru diperkenalkan di versi 2.0. x tidak kompatibel ke belakang. Untuk memperbarui dari versi lebih awal dari 1.7. x ke versi 2.0. x dan yang lebih baru, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi AWS Encryption SDK. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

Anda dapat menginstal dengan cara berikut. AWS Encryption SDK for Java

Secara manual

Untuk menginstal AWS Encryption SDK for Java, kloning atau unduh aws-encryption-sdk-java GitHubrepositori.

Menggunakan Apache Maven

AWS Encryption SDK for Java Ini tersedia melalui Apache Maven dengan definisi ketergantungan berikut.

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-encryption-sdk-java</artifactId>
  <version>3.0.0</version>
</dependency>
```

Setelah Anda menginstal SDK, mulailah dengan melihat contoh kode Java dalam panduan ini dan Javadoc aktif. GitHub

AWS Encryption SDK for Java contoh

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK for Java mendekripsi data. Contoh-contoh ini menunjukkan cara menggunakan versi 3. x dan yang lebih baru AWS Encryption SDK for Java. Versi 3. x dari yang AWS Encryption SDK for Java membutuhkan AWS SDK for Java 2.x. Versi 3. x dari AWS Encryption SDK for Java menggantikan penyedia kunci master dengan keyrings. Untuk contoh yang menggunakan versi sebelumnya, temukan rilis Anda di daftar Rilis aws-encryption-sdk-javarepositori di. GitHub

Topik

- Mengenkripsi dan mendekripsi string
- Mengenkripsi dan mendekripsi aliran byte
- Mengenkripsi dan mendekripsi aliran byte dengan multi-keyring

Mengenkripsi dan mendekripsi string

Contoh berikut menunjukkan cara menggunakan versi 3. x dari AWS Encryption SDK for Java untuk mengenkripsi dan mendekripsi string. Sebelum menggunakan string, ubah menjadi array byte.

Contoh ini menggunakan AWS KMS keyring. Saat Anda mengenkripsi dengan AWS KMS keyring, Anda dapat menggunakan ID kunci, ARN kunci, nama alias, atau alias ARN untuk mengidentifikasi kunci KMS. Saat mendekripsi, Anda harus menggunakan ARN kunci untuk mengidentifikasi kunci KMS.

Ketika Anda memanggil `encryptData()` metode, ia mengembalikan pesan terenkripsi (`CryptoResult`) yang mencakup ciphertext, kunci data terenkripsi, dan konteks enkripsi. Ketika Anda memanggil `getResult` `CryptoResult` objek, ia mengembalikan versi string yang dikodekan basis-64 dari pesan terenkripsi yang dapat Anda teruskan ke metode. `decryptData()`

Demikian pula, ketika Anda memanggil`decryptData()`, `CryptoResult` objek yang dikembalikan berisi pesan teks biasa AWS KMS key dan ID. Sebelum aplikasi Anda mengembalikan plaintext, verifikasi bahwa AWS KMS key ID dan konteks enkripsi dalam pesan terenkripsi adalah yang Anda harapkan.

```
// Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

package com.amazonaws.crypto.keyrings;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CommitmentPolicy;
import com.amazonaws.encryptionsdk.CryptoResult;
import software.amazon.cryptography.materialproviders.IKeyring;
import software.amazon.cryptography.materialproviders.MaterialProviders;
import
 software.amazon.cryptography.materialproviders.model.CreateAwsKmsMultiKeyringInput;
import software.amazon.cryptography.materialproviders.model.MaterialProvidersConfig;

import java.nio.charset.StandardCharsets;
import java.util.Arrays;
import java.util.Collections;
import java.util.Map;

/**
 * Encrypts and then decrypts data using an AWS KMS Keyring.
 *
 * <p>Arguments:
 *
 * <ol>
 *   <li>Key ARN: For help finding the Amazon Resource Name (ARN) of your AWS KMS
 customer master
```

```
 *       key (CMK), see 'Viewing Keys' at
 *       http://docs.aws.amazon.com/kms/latest/developerguide/viewing-keys.html
 * </ol>
 */
public class BasicEncryptionKeyringExample {

  private static final byte[] EXAMPLE_DATA = "Hello
 World".getBytes(StandardCharsets.UTF_8);

  public static void main(final String[] args) {
    final String keyArn = args[0];

    encryptAndDecryptWithKeyring(keyArn);
  }

  public static void encryptAndDecryptWithKeyring(final String keyArn) {
    // 1. Instantiate the SDK
    // This builds the AwsCrypto client with the RequireEncryptRequireDecrypt
 commitment policy,
    // which means this client only encrypts using committing algorithm suites and
 enforces
    // that the client will only decrypt encrypted messages that were created with a
 committing
    // algorithm suite.
    // This is the default commitment policy if you build the client with
    // `AwsCrypto.builder().build()`
    // or `AwsCrypto.standard()`.
    final AwsCrypto crypto =
        AwsCrypto.builder()
            .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
            .build();

    // 2. Create the AWS KMS keyring.
    // This example creates a multi keyring, which automatically creates the KMS
 client.
    final MaterialProviders materialProviders =
        MaterialProviders.builder()
            .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
            .build();
    final CreateAwsKmsMultiKeyringInput keyringInput =
        CreateAwsKmsMultiKeyringInput.builder().generator(keyArn).build();
    final IKeyring kmsKeyring =
 materialProviders.CreateAwsKmsMultiKeyring(keyringInput);
```

```
    // 3. Create an encryption context
    // We recommend using an encryption context whenever possible
    // to protect integrity. This sample uses placeholder values.
    // For more information see:
    // blogs.aws.amazon.com/security/post/Tx2LZ6WBJJANTNW/How-to-Protect-the-Integrity-
of-Your-Encrypted-Data-by-Using-AWS-Key-Management
    final Map<String, String> encryptionContext =
        Collections.singletonMap("ExampleContextKey", "ExampleContextValue");

    // 4. Encrypt the data
    final CryptoResult<byte[], ?> encryptResult =
        crypto.encryptData(kmsKeyring, EXAMPLE_DATA, encryptionContext);
    final byte[] ciphertext = encryptResult.getResult();

    // 5. Decrypt the data
    final CryptoResult<byte[], ?> decryptResult =
        crypto.decryptData(
            kmsKeyring,
            ciphertext,
            // Verify that the encryption context in the result contains the
            // encryption context supplied to the encryptData method
            encryptionContext);

    // 6. Verify that the decrypted plaintext matches the original plaintext
    assert Arrays.equals(decryptResult.getResult(), EXAMPLE_DATA);
  }
}
```

Mengenkripsi dan mendekripsi aliran byte

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK mendekripsi aliran byte.

Contoh ini menggunakan keyring Raw AES.

Saat mengenkripsi, contoh ini menggunakan `AwsCrypto.builder() .withEncryptionAlgorithm()` metode untuk menentukan rangkaian algoritma tanpa tanda tangan digital. Saat mendekripsi, untuk memastikan bahwa ciphertext tidak ditandatangani, contoh ini menggunakan metode ini. `createUnsignedMessageDecryptingStream()` `createUnsignedMessageDecryptingStream()`Metode, gagal jika menemukan ciphertext dengan tanda tangan digital.

Jika Anda mengenkripsi dengan rangkaian algoritme default, yang menyertakan tanda tangan digital, gunakan `createDecryptingStream()` metode ini sebagai gantinya, seperti yang ditunjukkan pada contoh berikutnya.

```
// Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

package com.amazonaws.crypto.keyrings;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CommitmentPolicy;
import com.amazonaws.encryptionsdk.CryptoAlgorithm;
import com.amazonaws.encryptionsdk.CryptoInputStream;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;
import com.amazonaws.util.IOUtils;
import software.amazon.cryptography.materialproviders.IKeyring;
import software.amazon.cryptography.materialproviders.MaterialProviders;
import software.amazon.cryptography.materialproviders.model.AesWrappingAlg;
import software.amazon.cryptography.materialproviders.model.CreateRawAesKeyringInput;
import software.amazon.cryptography.materialproviders.model.MaterialProvidersConfig;

import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.nio.ByteBuffer;
import java.security.SecureRandom;
import java.util.Collections;
import java.util.Map;
import javax.crypto.SecretKey;
import javax.crypto.spec.SecretKeySpec;


/**
 * <p>
 * Encrypts and then decrypts a file under a random key.
 *
 * <p>
 * Arguments:
 * <ol>
 * <li>Name of file containing plaintext data to encrypt
 * </ol>
 *
 * <p>
```

```
 * This program demonstrates using a standard Java {@link SecretKey} object as a {@link
 IKeyring} to
 * encrypt and decrypt streaming data.
 */
public class FileStreamingKeyringExample {
    private static String srcFile;

    public static void main(String[] args) throws IOException {
        srcFile = args[0];

        // In this example, we generate a random key. In practice,
        // you would get a key from an existing store
        SecretKey cryptoKey = retrieveEncryptionKey();

        // Create a Raw Aes Keyring using the random key and an AES-GCM encryption
 algorithm
        final MaterialProviders materialProviders = MaterialProviders.builder()
                .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
                .build();
        final CreateRawAesKeyringInput keyringInput =
 CreateRawAesKeyringInput.builder()
                .wrappingKey(ByteBuffer.wrap(cryptoKey.getEncoded()))
                .keyNamespace("Example")
                .keyName("RandomKey")
                .wrappingAlg(AesWrappingAlg.ALG_AES128_GCM_IV12_TAG16)
                .build();
        IKeyring keyring = materialProviders.CreateRawAesKeyring(keyringInput);

        // Instantiate the SDK.
        // This builds the AwsCrypto client with the RequireEncryptRequireDecrypt
 commitment policy,
        // which means this client only encrypts using committing algorithm suites and
 enforces
        // that the client will only decrypt encrypted messages that were created with
 a committing
        // algorithm suite.
        // This is the default commitment policy if you build the client with
        // `AwsCrypto.builder().build()`
        // or `AwsCrypto.standard()`.
        // This example encrypts with an algorithm suite that doesn't include signing
 for faster decryption,
        // since this use case assumes that the contexts that encrypt and decrypt are
 equally trusted.
        final AwsCrypto crypto = AwsCrypto.builder()
```

```
                .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)

.withEncryptionAlgorithm(CryptoAlgorithm.ALG_AES_256_GCM_HKDF_SHA512_COMMIT_KEY)
                .build();

        // Create an encryption context to identify the ciphertext
        Map<String, String> context = Collections.singletonMap("Example",
"FileStreaming");

        // Because the file might be too large to load into memory, we stream the data,
instead of
        //loading it all at once.
        FileInputStream in = new FileInputStream(srcFile);
        CryptoInputStream<JceMasterKey> encryptingStream =
crypto.createEncryptingStream(keyring, in, context);

        FileOutputStream out = new FileOutputStream(srcFile + ".encrypted");
        IOUtils.copy(encryptingStream, out);
        encryptingStream.close();
        out.close();

        // Decrypt the file. Verify the encryption context before returning the
plaintext.
        // Since the data was encrypted using an unsigned algorithm suite, use the
recommended
        // createUnsignedMessageDecryptingStream method, which only accepts unsigned
messages.
        in = new FileInputStream(srcFile + ".encrypted");
        CryptoInputStream<JceMasterKey> decryptingStream =
crypto.createUnsignedMessageDecryptingStream(keyring, in);
        // Does it contain the expected encryption context?
        if
(!"FileStreaming".equals(decryptingStream.getCryptoResult().getEncryptionContext().get("Exampl
{
            throw new IllegalStateException("Bad encryption context");
        }

        // Write the plaintext data to disk.
        out = new FileOutputStream(srcFile + ".decrypted");
        IOUtils.copy(decryptingStream, out);
        decryptingStream.close();
        out.close();
    }
```

```
    /**
     * In practice, this key would be saved in a secure location.
     * For this demo, we generate a new random key for each operation.
     */
    private static SecretKey retrieveEncryptionKey() {
        SecureRandom rnd = new SecureRandom();
        byte[] rawKey = new byte[16]; // 128 bits
        rnd.nextBytes(rawKey);
        return new SecretKeySpec(rawKey, "AES");
    }
}
```

Mengenkripsi dan mendekripsi aliran byte dengan multi-keyring

Contoh berikut menunjukkan cara menggunakan AWS Encryption SDK dengan multi-keyring. Bila Anda menggunakan multi-keyring untuk mengenkripsi data, salah satu kunci pembungkus di salah satu keyrings nya dapat mendekripsi data tersebut. Contoh ini menggunakan AWS KMS keyring dan keyring Raw RSA sebagai keyring anak.

Contoh ini mengenkripsi dengan rangkaian algoritme default, yang mencakup tanda tangan digital. Saat streaming, AWS Encryption SDK rilis plaintext setelah pemeriksaan integritas, tetapi sebelum memverifikasi tanda tangan digital. Untuk menghindari penggunaan plaintext sampai tanda tangan diverifikasi, contoh ini menyangga plaintext, dan menuliskannya ke disk hanya ketika dekripsi dan verifikasi selesai.

```
// Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

package com.amazonaws.crypto.keyrings;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CommitmentPolicy;
import com.amazonaws.encryptionsdk.CryptoOutputStream;
import com.amazonaws.util.IOUtils;
import software.amazon.cryptography.materialproviders.IKeyring;
import software.amazon.cryptography.materialproviders.MaterialProviders;
import
 software.amazon.cryptography.materialproviders.model.CreateAwsKmsMultiKeyringInput;
import software.amazon.cryptography.materialproviders.model.CreateMultiKeyringInput;
import software.amazon.cryptography.materialproviders.model.CreateRawRsaKeyringInput;
import software.amazon.cryptography.materialproviders.model.MaterialProvidersConfig;
import software.amazon.cryptography.materialproviders.model.PaddingScheme;
```

```
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.nio.ByteBuffer;
import java.security.GeneralSecurityException;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.util.Collections;

/**
 * <p>
 * Encrypts a file using both AWS KMS Key and an asymmetric key pair.
 *
 * <p>
 * Arguments:
 * <ol>
 * <li>Key ARN: For help finding the Amazon Resource Name (ARN) of your AWS KMS key,
 *   see 'Viewing Keys' at http://docs.aws.amazon.com/kms/latest/developerguide/
viewing-keys.html
 *
 * <li>Name of file containing plaintext data to encrypt
 * </ol>
 * <p>
 * You might use AWS Key Management Service (AWS KMS) for most encryption and
 decryption operations, but
 * still want the option of decrypting your data offline independently of AWS KMS. This
 sample
 * demonstrates one way to do this.
 * <p>
 * The sample encrypts data under both an AWS KMS key and an "escrowed" RSA key pair
 * so that either key alone can decrypt it. You might commonly use the AWS KMS key for
 decryption. However,
 * at any time, you can use the private RSA key to decrypt the ciphertext independent
 of AWS KMS.
 * <p>
 * This sample uses the RawRsaKeyring to generate a RSA public-private key pair
 * and saves the key pair in memory. In practice, you would store the private key in a
 secure offline
 * location, such as an offline HSM, and distribute the public key to your development
 team.
 */
public class EscrowedEncryptKeyringExample {
```

```
    private static ByteBuffer publicEscrowKey;
    private static ByteBuffer privateEscrowKey;

    public static void main(final String[] args) throws Exception {
        // This sample generates a new random key for each operation.
        // In practice, you would distribute the public key and save the private key in
secure
        // storage.
        generateEscrowKeyPair();

        final String kmsArn = args[0];
        final String fileName = args[1];

        standardEncrypt(kmsArn, fileName);
        standardDecrypt(kmsArn, fileName);

        escrowDecrypt(fileName);
    }

    private static void standardEncrypt(final String kmsArn, final String fileName)
throws Exception {
        // Encrypt with the KMS key and the escrowed public key
        // 1. Instantiate the SDK
        // This builds the AwsCrypto client with the RequireEncryptRequireDecrypt
commitment policy,
        // which means this client only encrypts using committing algorithm suites and
enforces
        // that the client will only decrypt encrypted messages that were created with
a committing
        // algorithm suite.
        // This is the default commitment policy if you build the client with
        // `AwsCrypto.builder().build()`
        // or `AwsCrypto.standard()`.
        final AwsCrypto crypto = AwsCrypto.builder()
                .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
                .build();

        // 2. Create the AWS KMS keyring.
        // This example creates a multi keyring, which automatically creates the KMS
client.
        final MaterialProviders matProv = MaterialProviders.builder()
                .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
                .build();
```

```
        final CreateAwsKmsMultiKeyringInput keyringInput =
CreateAwsKmsMultiKeyringInput.builder()
                .generator(kmsArn)
                .build();
        IKeyring kmsKeyring = matProv.CreateAwsKmsMultiKeyring(keyringInput);

        // 3. Create the Raw Rsa Keyring with Public Key.
        final CreateRawRsaKeyringInput encryptingKeyringInput =
CreateRawRsaKeyringInput.builder()
                .keyName("Escrow")
                .keyNamespace("Escrow")
                .paddingScheme(PaddingScheme.OAEP_SHA512_MGF1)
                .publicKey(publicEscrowKey)
                .build();
        IKeyring rsaPublicKeyring =
matProv.CreateRawRsaKeyring(encryptingKeyringInput);

        // 4. Create the multi-keyring.
        final CreateMultiKeyringInput createMultiKeyringInput =
CreateMultiKeyringInput.builder()
                .generator(kmsKeyring)
                .childKeyrings(Collections.singletonList(rsaPublicKeyring))
                .build();
        IKeyring multiKeyring = matProv.CreateMultiKeyring(createMultiKeyringInput);

        // 5. Encrypt the file
        // To simplify this code example, we omit the encryption context. Production
code should always
        // use an encryption context.
        final FileInputStream in = new FileInputStream(fileName);
        final FileOutputStream out = new FileOutputStream(fileName + ".encrypted");
        final CryptoOutputStream<?> encryptingStream =
crypto.createEncryptingStream(multiKeyring, out);

        IOUtils.copy(in, encryptingStream);
        in.close();
        encryptingStream.close();
    }

    private static void standardDecrypt(final String kmsArn, final String fileName)
throws Exception {
        // Decrypt with the AWS KMS key and the escrow public key.

        // 1. Instantiate the SDK.
```

```
        // This builds the AwsCrypto client with the RequireEncryptRequireDecrypt
commitment policy,
        // which means this client only encrypts using committing algorithm suites and
enforces
        // that the client will only decrypt encrypted messages that were created with
a committing
        // algorithm suite.
        // This is the default commitment policy if you build the client with
        // `AwsCrypto.builder().build()`
        // or `AwsCrypto.standard()`.
        final AwsCrypto crypto = AwsCrypto.builder()
                .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
                .build();

        // 2. Create the AWS KMS keyring.
        // This example creates a multi keyring, which automatically creates the KMS
client.
        final MaterialProviders matProv = MaterialProviders.builder()
                .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
                .build();
        final CreateAwsKmsMultiKeyringInput keyringInput =
CreateAwsKmsMultiKeyringInput.builder()
                .generator(kmsArn)
                .build();
        IKeyring kmsKeyring = matProv.CreateAwsKmsMultiKeyring(keyringInput);

        // 3. Create the Raw Rsa Keyring with Public Key.
        final CreateRawRsaKeyringInput encryptingKeyringInput =
CreateRawRsaKeyringInput.builder()
                .keyName("Escrow")
                .keyNamespace("Escrow")
                .paddingScheme(PaddingScheme.OAEP_SHA512_MGF1)
                .publicKey(publicEscrowKey)
                .build();
        IKeyring rsaPublicKeyring =
matProv.CreateRawRsaKeyring(encryptingKeyringInput);

        // 4. Create the multi-keyring.
        final CreateMultiKeyringInput createMultiKeyringInput =
CreateMultiKeyringInput.builder()
                .generator(kmsKeyring)
                .childKeyrings(Collections.singletonList(rsaPublicKeyring))
                .build();
        IKeyring multiKeyring = matProv.CreateMultiKeyring(createMultiKeyringInput);
```

```
        // 5. Decrypt the file
        // To simplify this code example, we omit the encryption context. Production
code should always
        // use an encryption context.
        final FileInputStream in = new FileInputStream(fileName + ".encrypted");
        final FileOutputStream out = new FileOutputStream(fileName + ".decrypted");
        // Since we are using a signing algorithm suite, we avoid streaming decryption
directly to the output file,
        // to ensure that the trailing signature is verified before writing any
untrusted plaintext to disk.
        final ByteArrayOutputStream plaintextBuffer = new ByteArrayOutputStream();
        final CryptoOutputStream<?> decryptingStream =
crypto.createDecryptingStream(multiKeyring, plaintextBuffer);
        IOUtils.copy(in, decryptingStream);
        in.close();
        decryptingStream.close();
        final ByteArrayInputStream plaintextReader = new
ByteArrayInputStream(plaintextBuffer.toByteArray());
        IOUtils.copy(plaintextReader, out);
        out.close();
    }

    private static void escrowDecrypt(final String fileName) throws Exception {
        // You can decrypt the stream using only the private key.
        // This method does not call AWS KMS.

        // 1. Instantiate the SDK
        final AwsCrypto crypto = AwsCrypto.standard();

        // 2. Create the Raw Rsa Keyring with Private Key.
        final MaterialProviders matProv = MaterialProviders.builder()
                .MaterialProvidersConfig(MaterialProvidersConfig.builder().build())
                .build();
        final CreateRawRsaKeyringInput encryptingKeyringInput =
CreateRawRsaKeyringInput.builder()
                .keyName("Escrow")
                .keyNamespace("Escrow")
                .paddingScheme(PaddingScheme.OAEP_SHA512_MGF1)
                .publicKey(publicEscrowKey)
                .privateKey(privateEscrowKey)
                .build();
        IKeyring escrowPrivateKeyring =
matProv.CreateRawRsaKeyring(encryptingKeyringInput);
```

```
        // 3. Decrypt the file
        // To simplify this code example, we omit the encryption context. Production
 code should always
        // use an encryption context.
        final FileInputStream in = new FileInputStream(fileName + ".encrypted");
        final FileOutputStream out = new FileOutputStream(fileName + ".deescrowed");
        final CryptoOutputStream<?> decryptingStream =
 crypto.createDecryptingStream(escrowPrivateKeyring, out);
        IOUtils.copy(in, decryptingStream);
        in.close();
        decryptingStream.close();

    }

    private static void generateEscrowKeyPair() throws GeneralSecurityException {
        final KeyPairGenerator kg = KeyPairGenerator.getInstance("RSA");
        kg.initialize(4096); // Escrow keys should be very strong
        final KeyPair keyPair = kg.generateKeyPair();
        publicEscrowKey = RawRsaKeyringExample.getPEMPublicKey(keyPair.getPublic());
        privateEscrowKey = RawRsaKeyringExample.getPEMPrivateKey(keyPair.getPrivate());

    }
}
```

AWS Encryption SDK for JavaScript

AWS Encryption SDK for JavaScript Ini dirancang untuk menyediakan pustaka enkripsi sisi klien untuk pengembang yang menulis aplikasi browser web di JavaScript atau aplikasi server web di Node.js.

Seperti semua implementasi AWS Encryption SDK, AWS Encryption SDK for JavaScript menawarkan fitur perlindungan data tingkat lanjut. Ini termasuk enkripsi amplop, data otentikasi tambahan (AAD), dan rangkaian algoritma kunci simetris yang aman, diautentikasi, seperti AES-GCM 256-bit dengan derivasi dan penandatanganan kunci.

Semua implementasi khusus bahasa dirancang agar dapat dioperasikan, tunduk pada kendala bahasa. AWS Encryption SDK Untuk detail tentang batasan bahasa, lihat. JavaScript the section called “Kompatibilitas”

Pelajari Lebih Lanjut

- Untuk detail tentang pemrograman dengan AWS Encryption SDK for JavaScript, lihat aws-encryption-sdk-javascriptrepositori di. GitHub
- Untuk contoh pemrograman, lihat the section called “Contoh” dan modul example-browser dan example-node di repositori. aws-encryption-sdk-javascript
- Untuk contoh dunia nyata menggunakan data AWS Encryption SDK for JavaScript untuk mengenkripsi dalam aplikasi web, lihat Cara mengaktifkan enkripsi di browser dengan AWS Encryption SDK for JavaScript dan Node.js di Blog AWS Keamanan.

Topik

Kompatibilitas AWS Encryption SDK for JavaScript

AWS Encryption SDK for JavaScript Ini dirancang untuk dapat dioperasikan dengan implementasi bahasa lain dari. AWS Encryption SDK Dalam kebanyakan kasus, Anda dapat mengenkripsi data dengan AWS Encryption SDK for JavaScript dan mendekripsi dengan implementasi bahasa lain, termasuk Antarmuka Baris AWS Encryption SDK Perintah. Dan Anda dapat menggunakan AWS Encryption SDK for JavaScript untuk mendekripsi pesan terenkripsi yang dihasilkan oleh implementasi bahasa lain dari. AWS Encryption SDK

Namun, ketika Anda menggunakan AWS Encryption SDK for JavaScript, Anda perlu menyadari beberapa masalah kompatibilitas dalam implementasi JavaScript bahasa dan di browser web.

Selain itu, saat menggunakan implementasi bahasa yang berbeda, pastikan untuk mengonfigurasi penyedia kunci master, kunci master, dan gantungan kunci yang kompatibel. Lihat perinciannya di Kompatibilitas keyring.

AWS Encryption SDK for JavaScript kompatibilitas

JavaScript Implementasi AWS Encryption SDK berbeda dari implementasi bahasa lain dengan cara berikut:

- Operasi enkripsi AWS Encryption SDK for JavaScript tidak mengembalikan ciphertext nonframed. Namun, AWS Encryption SDK for JavaScript wasiat mendekripsi ciphertext berbingkai dan tidak dibingkai yang dikembalikan oleh implementasi bahasa lain dari. AWS Encryption SDK
- Mulai dari Node.js versi 12.9.0, Node.js mendukung opsi pembungkus kunci RSA berikut:
  - OAEP dengan SHA1,, SHA256, SHA384 atau SHA512
  - OAEP dengan dan dengan SHA1 MGF1 SHA1
  - PKCS1v15
- Sebelum versi 12.9.0, Node.js hanya mendukung opsi pembungkus kunci RSA berikut:
  - OAEP dengan dan dengan SHA1 MGF1 SHA1
  - PKCS1v15

Kompabilitas peramban

Beberapa browser web tidak mendukung operasi kriptografi dasar yang AWS Encryption SDK for JavaScript diperlukan. Anda dapat mengkompensasi beberapa operasi yang hilang dengan mengonfigurasi fallback untuk WebCrypto API yang diterapkan browser.

Keterbatasan browser web

Keterbatasan berikut umum untuk semua browser web:

- WebCrypto API tidak mendukung pembungkus PKCS1v15 kunci.
- Browser tidak mendukung kunci 192-bit.

Operasi kriptografi yang diperlukan

Ini AWS Encryption SDK for JavaScript membutuhkan operasi berikut di browser web. Jika browser tidak mendukung operasi ini, itu tidak kompatibel dengan. AWS Encryption SDK for JavaScript

- Browser harus menyertakan`crypto.getRandomValues()`, yang merupakan metode untuk menghasilkan nilai acak kriptografis. Untuk informasi tentang versi browser web yang mendukung`crypto.getRandomValues()`, lihat Dapatkah Saya Menggunakan kripto. getRandomValues()? .

Fallback yang dibutuhkan

Ini AWS Encryption SDK for JavaScript membutuhkan perpustakaan dan operasi berikut di browser web. Jika Anda mendukung browser web yang tidak memenuhi persyaratan ini, Anda harus mengonfigurasi fallback. Jika tidak, upaya untuk AWS Encryption SDK for JavaScript menggunakan browser akan gagal.

- WebCrypto API, yang melakukan operasi kriptografi dasar dalam aplikasi web, tidak tersedia untuk semua browser. Untuk informasi tentang versi browser web yang mendukung kriptografi web, lihat Dapatkah Saya Menggunakan Kriptografi Web? .
- Versi modern dari browser web Safari tidak mendukung enkripsi AES-GCM nol byte, yang diperlukan. AWS Encryption SDK Jika browser mengimplementasikan WebCrypto API, tetapi tidak dapat menggunakan AES-GCM untuk mengenkripsi nol byte, browser AWS Encryption SDK for JavaScript menggunakan pustaka fallback hanya untuk enkripsi nol-byte. Ini menggunakan WebCrypto API untuk semua operasi lainnya.

Untuk mengonfigurasi fallback untuk salah satu batasan, tambahkan pernyataan berikut ke kode Anda. Dalam fungsi ConfigurefallBack, tentukan pustaka yang mendukung fitur yang hilang. Contoh berikut menggunakan Microsoft Research JavaScript Cryptography Library (`msrcrypto`), tetapi Anda dapat menggantinya dengan perpustakaan yang kompatibel. Untuk contoh lengkapnya, lihat fallback.ts.

```
import { configureFallback } from '@aws-crypto/client-browser'
configureFallback(msrCrypto)
```

Memasang AWS Encryption SDK for JavaScript

AWS Encryption SDK for JavaScript Terdiri dari kumpulan modul yang saling bergantung. Beberapa modul hanyalah kumpulan modul yang dirancang untuk bekerja sama. Beberapa modul dirancang untuk bekerja secara mandiri. Beberapa modul diperlukan untuk semua implementasi; beberapa lainnya hanya diperlukan untuk kasus khusus. Untuk informasi tentang modul di AWS Encryption SDK for JavaScript, lihat Modul di AWS Encryption SDK for JavaScript dan `README.md` file di masing-masing modul di aws-encryption-sdk-javascriptrepositori pada. GitHub

> **Note**
>
> Semua versi yang AWS Encryption SDK for JavaScript lebih awal dari 2.0.0 sedang dalam fase. end-of-support

Anda dapat memperbarui dengan aman dari versi 2.0. x dan yang lebih baru ke versi terbaru AWS Encryption SDK for JavaScript tanpa kode atau perubahan data. Namun, fitur keamanan baru diperkenalkan di versi 2.0. x tidak kompatibel ke belakang. Untuk memperbarui dari versi lebih awal dari 1.7. x ke versi 2.0. x dan yang lebih baru, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi AWS Encryption SDK for JavaScript. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

Untuk menginstal modul, gunakan manajer paket npm.

Misalnya, untuk menginstal `client-node` modul, yang mencakup semua modul yang Anda butuhkan untuk memprogram dengan AWS Encryption SDK for JavaScript di Node.js, gunakan perintah berikut.

```
npm install @aws-crypto/client-node
```

Untuk menginstal `client-browser` modul, yang mencakup semua modul yang perlu Anda program dengan AWS Encryption SDK for JavaScript di browser, gunakan perintah berikut.

```
npm install @aws-crypto/client-browser
```

Untuk contoh kerja tentang cara menggunakan AWS Encryption SDK for JavaScript, lihat contoh di `example-node` dan `example-browser` modul di aws-encryption-sdk-javascriptrepositori pada. GitHub

Modul di AWS Encryption SDK for JavaScript

Modul di AWS Encryption SDK for JavaScript membuatnya mudah untuk menginstal kode yang Anda butuhkan untuk proyek Anda.

Modul untuk JavaScript Node.js

simpul klien

Termasuk semua modul yang Anda butuhkan untuk memprogram dengan AWS Encryption SDK for JavaScript di Node.js.

caching-materials-manager-node

Mengekspor fungsi yang mendukung fitur caching kunci data AWS Encryption SDK for JavaScript di Node.js.

dekripsi-simpul

Mengekspor fungsi yang mendekripsi dan memverifikasi pesan terenkripsi yang mewakili aliran data dan data. Termasuk dalam `client-node` modul.

enkripsi-simpul

Mengekspor fungsi yang mengenkripsi dan menandatangani berbagai jenis data. Termasuk dalam `client-node` modul.

contoh-simpul

Mengekspor contoh kerja pemrograman dengan AWS Encryption SDK for JavaScript di Node.js. Termasuk contoh berbagai jenis gantungan kunci dan berbagai jenis data.

hkdf-simpul

Mengekspor Fungsi Derivasi Kunci (HKDF) berbasis HMAC yang digunakan di Node.js AWS Encryption SDK for JavaScript dalam rangkaian algoritma tertentu. AWS Encryption SDK for JavaScript Di browser menggunakan fungsi HKDF asli di API. WebCrypto

integrasi-simpul

Mendefinisikan pengujian yang memverifikasi bahwa AWS Encryption SDK for JavaScript di Node.js kompatibel dengan implementasi bahasa lain dari file. AWS Encryption SDK

kms-keyring-node

Mengekspor fungsi yang mendukung AWS KMS keyrings di Node.js.

raw-aes-keyring-node

Mengekspor fungsi yang mendukung keyrings Raw AES di Node.js.

raw-rsa-keyring-node

Mengekspor fungsi yang mendukung keyring Raw RSA di Node.js.

Modul untuk JavaScript Browser

[peramban klien]

Termasuk semua modul yang Anda butuhkan untuk memprogram dengan AWS Encryption SDK for JavaScript di browser.

[caching-materials-manager-browser]

Mengekspor fungsi yang mendukung fitur caching kunci data untuk JavaScript di browser.

[dekripsi-browser]

Mengekspor fungsi yang mendekripsi dan memverifikasi pesan terenkripsi yang mewakili aliran data dan data.

[browser terenkripsi]

Mengekspor fungsi yang mengenkripsi dan menandatangani berbagai jenis data.

[contoh-browser]

Contoh kerja pemrograman dengan AWS Encryption SDK for JavaScript di browser. Termasuk contoh berbagai jenis gantungan kunci dan berbagai jenis data.

[integrasi-browser]

Mendefinisikan tes yang memverifikasi bahwa AWS Encryption SDK for Java Script di browser kompatibel dengan implementasi bahasa lain dari file. AWS Encryption SDK

[kms-keyring-browser]

Mengekspor fungsi yang mendukung AWS KMS keyrings di browser.

[raw-aes-keyring-browser]

Mengekspor fungsi yang mendukung keyrings Raw AES di browser.

[raw-rsa-keyring-browser]

Mengekspor fungsi yang mendukung keyring Raw RSA di browser.

Modul untuk semua implementasi

[bahan tembolok]

Mendukung fitur caching kunci data. Menyediakan kode untuk merakit materi kriptografi yang di-cache dengan setiap kunci data.

kms-keyring

Mengekspor fungsi yang mendukung keyrings KMS.

manajemen material

Menerapkan manajer bahan kriptografi (CMM).

gantungan kunci mentah

Fungsi ekspor diperlukan untuk gantungan kunci AES dan RSA mentah.

serialisasi

Mengekspor fungsi yang digunakan SDK untuk membuat serial outputnya.

web-crypto-backend

Mengekspor fungsi yang menggunakan WebCrypto API AWS Encryption SDK for JavaScript di browser.

AWS Encryption SDK for JavaScript contoh

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK for JavaScript mendekripsi data.

Anda dapat menemukan lebih banyak contoh penggunaan modul example-node dan example-browser AWS Encryption SDK for JavaScript di repositori pada. aws-encryption-sdk-javascript GitHub Modul contoh ini tidak diinstal ketika Anda menginstal `client-browser` atau `client-node` modul.

Lihat contoh kode lengkap: Node: kms_simple.ts, Browser: kms_simple.ts

Topik

- Mengenkripsi data dengan keyring AWS KMS
- Mendekripsi data dengan keyring AWS KMS

Mengenkripsi data dengan keyring AWS KMS

Contoh berikut menunjukkan kepada Anda bagaimana menggunakan AWS Encryption SDK for JavaScript untuk mengenkripsi dan mendekripsi string pendek atau array byte.

Contoh ini menampilkan AWS KMS keyring, jenis keyring yang menggunakan AWS KMS key untuk menghasilkan dan mengenkripsi kunci data. Untuk bantuan membuat AWS KMS key, lihat Membuat

Kunci di Panduan AWS Key Management Service Pengembang. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihat Mengidentifikasi AWS KMS keys dalam AWS KMS keyring

Langkah 1: Tetapkan kebijakan komitmen.

Dimulai pada versi 1.7. x dari AWS Encryption SDK for JavaScript, Anda dapat mengatur kebijakan komitmen ketika Anda memanggil `buildClient` fungsi baru yang membuat instance AWS Encryption SDK klien. `buildClient`Fungsi ini mengambil nilai yang disebutkan yang mewakili kebijakan komitmen Anda. Ini mengembalikan `decrypt` fungsi yang diperbarui `encrypt` dan memberlakukan kebijakan komitmen Anda saat Anda mengenkripsi dan mendekripsi.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called “Membatasi kunci data terenkripsi”.

JavaScript Browser

```
import {
  KmsKeyringBrowser,
  KMS,
  getClient,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-browser'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)
```

JavaScript Node.js

```
import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
```

```
)
```

Langkah 2: Bangun keyring.

Buat AWS KMS keyring untuk enkripsi.

Saat mengenkripsi dengan AWS KMS keyring, Anda harus menentukan kunci generator, yaitu kunci yang digunakan untuk menghasilkan kunci data plaintext dan mengenkripsinya. AWS KMS key Anda juga dapat menentukan nol atau lebih kunci tambahan yang mengenkripsi kunci data teks biasa yang sama. Keyring mengembalikan kunci data plaintext dan satu salinan terenkripsi dari kunci data tersebut untuk masing-masing AWS KMS key di keyring, termasuk kunci generator. Untuk mendekripsi data, Anda perlu mendekripsi salah satu kunci data terenkripsi.

Untuk menentukan keyring enkripsi di dalam AWS Encryption SDK for JavaScript, Anda dapat menggunakan pengenal AWS KMS kunci yang didukung. AWS KMS keys Contoh ini menggunakan kunci generator, yang diidentifikasi oleh alias ARN, dan satu kunci tambahan, yang diidentifikasi oleh ARN kunci.

> **Note**
>
> Jika Anda berencana untuk menggunakan kembali AWS KMS keyring Anda untuk mendekripsi, Anda harus menggunakan kunci ARNs untuk mengidentifikasi di AWS KMS keys keyring.

Sebelum menjalankan kode ini, ganti AWS KMS key pengidentifikasi contoh dengan pengidentifikasi yang valid. Anda harus memiliki izin yang diperlukan untuk menggunakan AWS KMS keys di keyring.

JavaScript Browser

Mulailah dengan memberikan kredensil Anda ke browser. AWS Encryption SDK for JavaScript Contohnya menggunakan webpack. DefinePlugin, yang menggantikan konstanta kredenal dengan kredensil Anda yang sebenarnya. Tetapi Anda dapat menggunakan metode apa pun untuk memberikan kredensil Anda. Kemudian, gunakan kredensialnya untuk membuat klien. AWS KMS

```
declare const credentials: {accessKeyId: string, secretAccessKey:string,
 sessionToken:string }
```

```
const clientProvider = getClient(KMS, {
  credentials: {
    accessKeyId,
    secretAccessKey,
    sessionToken
  }
})
```

Selanjutnya, tentukan AWS KMS keys untuk kunci generator dan kunci tambahan. Kemudian, buat AWS KMS keyring menggunakan AWS KMS klien dan. AWS KMS keys

```
const generatorKeyId = 'arn:aws:kms:us-west-2:111122223333:alias/EncryptDecrypt'
const keyIds = ['arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab']

const keyring = new KmsKeyringBrowser({ clientProvider, generatorKeyId, keyIds })
```

JavaScript Node.js

```
const generatorKeyId = 'arn:aws:kms:us-west-2:111122223333:alias/EncryptDecrypt'
const keyIds = ['arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab']

const keyring = new KmsKeyringNode({ generatorKeyId, keyIds })
```

Langkah 3: Atur konteks enkripsi.

Konteks enkripsi adalah data otentikasi tambahan yang sewenang-wenang dan tidak rahasia. Ketika Anda menyediakan konteks enkripsi pada enkripsi, AWS Encryption SDK kriptografis mengikat konteks enkripsi ke ciphertext sehingga konteks enkripsi yang sama diperlukan untuk mendekripsi data. Menggunakan konteks enkripsi adalah opsional, tetapi kami merekomendasikannya sebagai praktik terbaik.

Buat objek sederhana yang mencakup pasangan konteks enkripsi. Kunci dan nilai dalam setiap pasangan harus berupa string.

JavaScript Browser

```
const context = {
  stage: 'demo',
  purpose: 'simple demonstration app',
```

```
  origin: 'us-west-2'
}
```

JavaScript Node.js

```
const context = {
  stage: 'demo',
  purpose: 'simple demonstration app',
  origin: 'us-west-2'
}
```

Langkah 4: Enkripsi data.

Untuk mengenkripsi data plaintext, panggil fungsi. `encrypt` Masukkan AWS KMS keyring, data plaintext, dan konteks enkripsi.

`encrypt`Fungsi mengembalikan pesan terenkripsi (`result`) yang berisi data terenkripsi, kunci data terenkripsi, dan metadata penting, termasuk konteks enkripsi dan tanda tangan.

Anda dapat mendekripsi pesan terenkripsi ini dengan menggunakan AWS Encryption SDK untuk bahasa pemrograman yang didukung.

JavaScript Browser

```
const plaintext = new Uint8Array([1, 2, 3, 4, 5])

const { result } = await encrypt(keyring, plaintext, { encryptionContext:
 context })
```

JavaScript Node.js

```
const plaintext = 'asdf'

const { result } = await encrypt(keyring, plaintext, { encryptionContext:
 context })
```

Mendekripsi data dengan keyring AWS KMS

Anda dapat menggunakan AWS Encryption SDK for JavaScript untuk mendekripsi pesan terenkripsi dan memulihkan data asli.

Dalam contoh ini, kami mendekripsi data yang kami enkripsi dalam contoh. the section called "Mengenkripsi data dengan keyring AWS KMS"

Langkah 1: Tetapkan kebijakan komitmen.

Dimulai pada versi 1.7. x dari AWS Encryption SDK for JavaScript, Anda dapat mengatur kebijakan komitmen ketika Anda memanggil `buildClient` fungsi baru yang membuat instance AWS Encryption SDK klien. `buildClient`Fungsi ini mengambil nilai yang disebutkan yang mewakili kebijakan komitmen Anda. Ini mengembalikan `decrypt` fungsi yang diperbarui `encrypt` dan memberlakukan kebijakan komitmen Anda saat Anda mengenkripsi dan mendekripsi.

Contoh berikut menggunakan `buildClient` fungsi untuk menentukan kebijakan komitmen default,`REQUIRE_ENCRYPT_REQUIRE_DECRYPT`. Anda juga dapat menggunakan `buildClient` untuk membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Untuk informasi selengkapnya, lihat the section called "Membatasi kunci data terenkripsi".

JavaScript Browser

```
import {
  KmsKeyringBrowser,
  KMS,
  getClient,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-browser'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)
```

JavaScript Node.js

```
import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
} from '@aws-crypto/client-node'

const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)
```

Langkah 2: Bangun keyring.

Untuk mendekripsi data, masukkan pesan terenkripsi (`result`) yang dikembalikan fungsi. `encrypt` Pesan terenkripsi mencakup data terenkripsi, kunci data terenkripsi, dan metadata penting, termasuk konteks enkripsi dan tanda tangan.

Anda juga harus menentukan AWS KMS keyring saat mendekripsi. Anda dapat menggunakan keyring yang sama yang digunakan untuk mengenkripsi data atau keyring yang berbeda. Agar berhasil, setidaknya satu AWS KMS key di keyring dekripsi harus dapat mendekripsi salah satu kunci data terenkripsi dalam pesan terenkripsi. Karena tidak ada kunci data yang dihasilkan, Anda tidak perlu menentukan kunci generator dalam keyring dekripsi. Jika Anda melakukannya, kunci generator dan kunci tambahan diperlakukan dengan cara yang sama.

Untuk menentukan AWS KMS key untuk keyring dekripsi di AWS Encryption SDK for JavaScript, Anda harus menggunakan kunci ARN. Kalau tidak, AWS KMS key tidak dikenali. Untuk bantuan mengidentifikasi AWS KMS keys dalam AWS KMS gantungan kunci, lihat Mengidentifikasi AWS KMS keys dalam AWS KMS keyring

> **Note**
>
> Jika Anda menggunakan keyring yang sama untuk mengenkripsi dan mendekripsi, gunakan kunci ARNs untuk mengidentifikasi di keyring. AWS KMS keys

Dalam contoh ini, kami membuat keyring yang hanya menyertakan salah satu dari keyring enkripsi. AWS KMS keys Sebelum menjalankan kode ini, ganti contoh kunci ARN dengan yang valid. Anda harus memiliki `kms:Decrypt` izin pada AWS KMS key.

JavaScript Browser

Mulailah dengan memberikan kredensil Anda ke browser. AWS Encryption SDK for JavaScript Contohnya menggunakan webpack. DefinePlugin, yang menggantikan konstanta kredenal dengan kredensil Anda yang sebenarnya. Tetapi Anda dapat menggunakan metode apa pun untuk memberikan kredensil Anda. Kemudian, gunakan kredensialnya untuk membuat klien. AWS KMS

```
declare const credentials: {accessKeyId: string, secretAccessKey:string,
 sessionToken:string }

const clientProvider = getClient(KMS, {
```

```
  credentials: {
    accessKeyId,
    secretAccessKey,
    sessionToken
  }
})
```

Selanjutnya, buat AWS KMS keyring menggunakan AWS KMS klien. Contoh ini hanya menggunakan salah satu AWS KMS keys dari keyring enkripsi.

```
const keyIds = ['arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab']

const keyring = new KmsKeyringBrowser({ clientProvider, keyIds })
```

JavaScript Node.js

```
const keyIds = ['arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab']

const keyring = new KmsKeyringNode({ keyIds })
```

Langkah 3: Dekripsi data.

Selanjutnya, panggil `decrypt` fungsinya. Masukkan keyring dekripsi yang baru saja Anda buat (`keyring`) dan pesan terenkripsi yang dikembalikan oleh fungsi (). `encrypt` `result` AWS Encryption SDK Menggunakan keyring untuk mendekripsi salah satu kunci data terenkripsi. Kemudian menggunakan kunci data plaintext untuk mendekripsi data.

Jika panggilan berhasil, `plaintext` bidang berisi data plaintext (didekripsi). `messageHeader`Bidang berisi metadata tentang proses dekripsi, termasuk konteks enkripsi yang digunakan untuk mendekripsi data.

JavaScript Browser

```
const { plaintext, messageHeader } = await decrypt(keyring, result)
```

JavaScript Node.js

```
const { plaintext, messageHeader } = await decrypt(keyring, result)
```

Langkah 4: Verifikasi konteks enkripsi.

Konteks enkripsi yang digunakan untuk mendekripsi data disertakan dalam header pesan (`messageHeader`) yang dikembalikan `decrypt` fungsi. Sebelum aplikasi Anda mengembalikan data plaintext, verifikasi bahwa konteks enkripsi yang Anda berikan saat mengenkripsi disertakan dalam konteks enkripsi yang digunakan saat mendekripsi. Ketidakcocokan mungkin menunjukkan bahwa data telah dirusak, atau bahwa Anda tidak mendekripsi ciphertext yang tepat.

Saat memverifikasi konteks enkripsi, tidak memerlukan kecocokan persis. Saat Anda menggunakan algoritma enkripsi dengan penandatanganan, pengelola materi kriptografi (CMM) menambahkan kunci penandatanganan publik ke konteks enkripsi sebelum mengenkripsi pesan. Tetapi semua pasangan konteks enkripsi yang Anda kirimkan harus disertakan dalam konteks enkripsi yang dikembalikan.

Pertama, dapatkan konteks enkripsi dari header pesan. Kemudian, verifikasi bahwa setiap pasangan kunci-nilai dalam konteks enkripsi asli (`context`) cocok dengan pasangan kunci-nilai dalam konteks enkripsi yang dikembalikan (). `encryptionContext`

JavaScript Browser

```
const { encryptionContext } = messageHeader

Object
  .entries(context)
  .forEach(([key, value]) => {
    if (encryptionContext[key] !== value) throw new Error('Encryption Context
 does not match expected values')
})
```

JavaScript Node.js

```
const { encryptionContext } = messageHeader

Object
  .entries(context)
  .forEach(([key, value]) => {
    if (encryptionContext[key] !== value) throw new Error('Encryption Context
 does not match expected values')
})
```

Jika pemeriksaan konteks enkripsi berhasil, Anda dapat mengembalikan data teks biasa.

AWS Encryption SDK for Python

Topik ini menjelaskan cara menginstal dan menggunakan AWS Encryption SDK for Python. Untuk detail tentang pemrograman dengan AWS Encryption SDK for Python, lihat aws-encryption-sdk-pythonrepositori di. GitHub Untuk dokumentasi API, lihat Membaca Dokumen.

Topik

Prasyarat

Sebelum Anda menginstal AWS Encryption SDK for Python, pastikan Anda memiliki prasyarat berikut.

Versi Python yang didukung

Python 3.8 atau yang lebih baru diperlukan oleh AWS Encryption SDK for Python versi 3.2.0 dan yang lebih baru.

> **Note**
>
> AWS Cryptographic Material Providers Library (MPL) adalah dependensi opsional untuk yang AWS Encryption SDK for Python diperkenalkan di versi 4. x. Jika Anda berniat menginstal MPL, Anda harus menggunakan Python 3.11 atau yang lebih baru.

Versi sebelumnya dari AWS Encryption SDK dukungan Python 2.7 dan Python 3.4 dan yang lebih baru, tetapi kami menyarankan Anda menggunakan versi terbaru dari versi. AWS Encryption SDK

Untuk mengunduh Python, lihat Unduh Python.

Alat instalasi pip untuk Python

`pip`termasuk dalam Python 3.6 dan versi yang lebih baru, meskipun Anda mungkin ingin memutakhirkannya. Untuk informasi selengkapnya tentang memutakhirkan atau menginstal`pip`, lihat Instalasi di `pip` dokumentasi.

Penginstalan

Instal versi terbaru dari file AWS Encryption SDK for Python.

> **Note**
>
> Semua versi yang AWS Encryption SDK for Python lebih awal dari 3.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.0. x dan yang lebih baru ke versi terbaru AWS Encryption SDK tanpa kode atau perubahan data. Namun, fitur keamanan baru diperkenalkan di versi 2.0. x tidak kompatibel ke belakang. Untuk memperbarui dari versi lebih awal dari 1.7. x ke versi 2.0. x dan yang lebih baru, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi AWS Encryption SDK. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

Gunakan `pip` untuk menginstal AWS Encryption SDK for Python, seperti yang ditunjukkan dalam contoh berikut.

Pasang versi terbaru

```
pip install "aws-encryption-sdk[MPL]"
```

`[MPL]`Akhiran menginstal Perpustakaan Penyedia Materi AWS Kriptografi (MPL). MPL berisi konstruksi untuk mengenkripsi dan mendekripsi data Anda. MPL adalah dependensi opsional untuk AWS Encryption SDK for Python diperkenalkan di versi 4. x. Kami sangat merekomendasikan menginstal MPL. Namun, jika Anda tidak berniat menggunakan MPL, Anda dapat menghilangkan akhiran. `[MPL]`

Untuk detail selengkapnya tentang penggunaan pip untuk menginstal dan memutakhirkan paket, lihat Menginstal Paket.

AWS Encryption SDK for Python Membutuhkan perpustakaan kriptografi (pyca/kriptografi) di semua platform. Semua versi menginstal dan membangun `cryptography` perpustakaan `pip` secara otomatis di Windows. `pip`8.1 dan yang lebih baru secara otomatis menginstal dan membangun `cryptography` di Linux. Jika Anda menggunakan versi sebelumnya `pip` dan lingkungan Linux Anda tidak memiliki alat yang diperlukan untuk membangun `cryptography` perpustakaan, Anda perlu menginstalnya. Untuk informasi selengkapnya, lihat Membangun Kriptografi di Linux.

Versi 1.10.0 dan 2.5.0 dari AWS Encryption SDK for Python pin ketergantungan kriptografi antara 2.5.0 dan 3.3.2. Versi lain dari AWS Encryption SDK for Python menginstal versi terbaru kriptografi. Jika Anda memerlukan versi kriptografi lebih lambat dari 3.3.2, kami sarankan Anda menggunakan versi utama terbaru dari. AWS Encryption SDK for Python

Untuk versi pengembangan terbaru AWS Encryption SDK for Python, buka aws-encryption-sdk-pythonrepositori di. GitHub

Setelah Anda menginstal AWS Encryption SDK for Python, mulailah dengan melihat kode contoh Python dalam panduan ini.

AWS Encryption SDK for Python kode contoh

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK for Python mendekripsi data.

Contoh di bagian ini menunjukkan cara menggunakan versi 4. x dari AWS Encryption SDK for Python dengan ketergantungan Perpustakaan Penyedia Materi Kriptografi opsional ()`aws-cryptographic-material-providers`. Untuk melihat contoh yang menggunakan versi sebelumnya, atau penginstalan tanpa pustaka penyedia materi (MPL), temukan rilis Anda di daftar Rilis aws-encryption-sdk-pythonrepositori di. GitHub

Bila Anda menggunakan versi 4. x dari AWS Encryption SDK for Python dengan MPL, ia menggunakan keyrings untuk melakukan enkripsi amplop. AWS Encryption SDK Ini menyediakan gantungan kunci yang kompatibel dengan penyedia kunci utama yang Anda gunakan di versi sebelumnya. Untuk informasi selengkapnya, lihat the section called “Kompatibilitas keyring”. Untuk contoh tentang migrasi dari penyedia kunci utama ke keyrings, lihat Contoh Migrasi di `aws-encryption-sdk-python` repositori pada; GitHub

Topik

- Mengenkripsi dan mendekripsi string
- Mengenkripsi dan mendekripsi aliran byte

Mengenkripsi dan mendekripsi string

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK mendekripsi string. Contoh ini menggunakan AWS KMS keyring dengan kunci KMS enkripsi simetris.

Contoh ini membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. REQUIRE_ENCRYPT_REQUIRE_DECRYPT Untuk informasi selengkapnya, lihat the section called "Menetapkan kebijakan komitmen Anda".

```
# Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
"""
This example sets up the KMS Keyring

The AWS KMS keyring uses symmetric encryption KMS keys to generate, encrypt and
decrypt data keys. This example creates a KMS Keyring and then encrypts a custom input
 EXAMPLE_DATA
with an encryption context. This example also includes some sanity checks for
 demonstration:
1. Ciphertext and plaintext data are not the same
2. Encryption context is correct in the decrypted message header
3. Decrypted plaintext value matches EXAMPLE_DATA
These sanity checks are for demonstration in the example only. You do not need these in
 your code.

AWS KMS keyrings can be used independently or in a multi-keyring with other keyrings
of the same or a different type.

"""

import boto3
from aws_cryptographic_material_providers.mpl import AwsCryptographicMaterialProviders
from aws_cryptographic_material_providers.mpl.config import MaterialProvidersConfig
from aws_cryptographic_material_providers.mpl.models import CreateAwsKmsKeyringInput
from aws_cryptographic_material_providers.mpl.references import IKeyring
from typing import Dict  # noqa pylint: disable=wrong-import-order

import aws_encryption_sdk
from aws_encryption_sdk import CommitmentPolicy

EXAMPLE_DATA: bytes = b"Hello World"


def encrypt_and_decrypt_with_keyring(
    kms_key_id: str
):
    """Demonstrate an encrypt/decrypt cycle using an AWS KMS keyring.
```

```
    Usage: encrypt_and_decrypt_with_keyring(kms_key_id)
    :param kms_key_id: KMS Key identifier for the KMS key you want to use for
encryption and
    decryption of your data keys.
    :type kms_key_id: string

    """
    # 1. Instantiate the encryption SDK client.
    # This builds the client with the REQUIRE_ENCRYPT_REQUIRE_DECRYPT commitment
policy,
    # which enforces that this client only encrypts using committing algorithm suites
and enforces
    # that this client will only decrypt encrypted messages that were created with a
committing
    # algorithm suite.
    # This is the default commitment policy if you were to build the client as
    # `client = aws_encryption_sdk.EncryptionSDKClient()`.
    client = aws_encryption_sdk.EncryptionSDKClient(
        commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
    )

    # 2. Create a boto3 client for KMS.
    kms_client = boto3.client('kms', region_name="us-west-2")

    # 3. Optional: create encryption context.
    # Remember that your encryption context is NOT SECRET.
    encryption_context: Dict[str, str] = {
        "encryption": "context",
        "is not": "secret",
        "but adds": "useful metadata",
        "that can help you": "be confident that",
        "the data you are handling": "is what you think it is",
    }

    # 4. Create your keyring
    mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
        config=MaterialProvidersConfig()
    )

    keyring_input: CreateAwsKmsKeyringInput = CreateAwsKmsKeyringInput(
        kms_key_id=kms_key_id,
        kms_client=kms_client
    )
```

```
    kms_keyring: IKeyring = mat_prov.create_aws_kms_keyring(
        input=keyring_input
    )

    # 5. Encrypt the data with the encryptionContext.
    ciphertext, _ = client.encrypt(
        source=EXAMPLE_DATA,
        keyring=kms_keyring,
        encryption_context=encryption_context
    )

    # 6. Demonstrate that the ciphertext and plaintext are different.
    # (This is an example for demonstration; you do not need to do this in your own
code.)
    assert ciphertext != EXAMPLE_DATA, \
        "Ciphertext and plaintext data are the same. Invalid encryption"

    # 7. Decrypt your encrypted data using the same keyring you used on encrypt.
    plaintext_bytes, _ = client.decrypt(
        source=ciphertext,
        keyring=kms_keyring,
        # Provide the encryption context that was supplied to the encrypt method
        encryption_context=encryption_context,
    )

    # 8. Demonstrate that the decrypted plaintext is identical to the original
plaintext.
    # (This is an example for demonstration; you do not need to do this in your own
code.)
    assert plaintext_bytes == EXAMPLE_DATA, \
        "Decrypted plaintext should be identical to the original plaintext. Invalid
decryption"
```

Mengenkripsi dan mendekripsi aliran byte

Contoh berikut menunjukkan cara menggunakan untuk mengenkripsi dan AWS Encryption SDK mendekripsi aliran byte. Contoh ini menggunakan keyring Raw AES.

Contoh ini membuat instance AWS Encryption SDK klien dengan kebijakan komitmen default,. `REQUIRE_ENCRYPT_REQUIRE_DECRYPT` Lihat informasi yang lebih lengkap di the section called “Menetapkan kebijakan komitmen Anda”.

```
# Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
```

```
# SPDX-License-Identifier: Apache-2.0
"""
This example demonstrates file streaming for encryption and decryption.

File streaming is useful when the plaintext or ciphertext file/data is too large to
 load into
memory. Therefore, the AWS Encryption SDK allows users to stream the data, instead of
 loading it
all at once in memory. In this example, we demonstrate file streaming for encryption
 and decryption
using a Raw AES keyring. However, you can use any keyring with streaming.

This example creates a Raw AES Keyring and then encrypts an input stream from the file
`plaintext_filename` with an encryption context to an output (encrypted) file
 `ciphertext_filename`.
It then decrypts the ciphertext from `ciphertext_filename` to a new file
 `decrypted_filename`.
This example also includes some sanity checks for demonstration:
1. Ciphertext and plaintext data are not the same
2. Encryption context is correct in the decrypted message header
3. Decrypted plaintext value matches EXAMPLE_DATA
These sanity checks are for demonstration in the example only. You do not need these in
 your code.

See raw_aes_keyring_example.py in the same directory for another raw AES keyring
 example
in the AWS Encryption SDK for Python.
"""
import filecmp
import secrets

from aws_cryptographic_material_providers.mpl import AwsCryptographicMaterialProviders
from aws_cryptographic_material_providers.mpl.config import MaterialProvidersConfig
from aws_cryptographic_material_providers.mpl.models import AesWrappingAlg,
 CreateRawAesKeyringInput
from aws_cryptographic_material_providers.mpl.references import IKeyring
from typing import Dict  # noqa pylint: disable=wrong-import-order

import aws_encryption_sdk
from aws_encryption_sdk import CommitmentPolicy


def encrypt_and_decrypt_with_keyring(
    plaintext_filename: str,
```

```
    ciphertext_filename: str,
    decrypted_filename: str
):
    """Demonstrate a streaming encrypt/decrypt cycle.

    Usage: encrypt_and_decrypt_with_keyring(plaintext_filename
                                            ciphertext_filename
                                            decrypted_filename)
    :param plaintext_filename: filename of the plaintext data
    :type plaintext_filename: string
    :param ciphertext_filename: filename of the ciphertext data
    :type ciphertext_filename: string
    :param decrypted_filename: filename of the decrypted data
    :type decrypted_filename: string
    """
    # 1. Instantiate the encryption SDK client.
    # This builds the client with the REQUIRE_ENCRYPT_REQUIRE_DECRYPT commitment
 policy,
    # which enforces that this client only encrypts using committing algorithm suites
 and enforces
    # that this client will only decrypt encrypted messages that were created with a
 committing
    # algorithm suite.
    # This is the default commitment policy if you were to build the client as
    # `client = aws_encryption_sdk.EncryptionSDKClient()`.
    client = aws_encryption_sdk.EncryptionSDKClient(
        commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
    )

    # 2. The key namespace and key name are defined by you.
    # and are used by the Raw AES keyring to determine
    # whether it should attempt to decrypt an encrypted data key.
    key_name_space = "Some managed raw keys"
    key_name = "My 256-bit AES wrapping key"

    # 3. Optional: create encryption context.
    # Remember that your encryption context is NOT SECRET.
    encryption_context: Dict[str, str] = {
        "encryption": "context",
        "is not": "secret",
        "but adds": "useful metadata",
        "that can help you": "be confident that",
        "the data you are handling": "is what you think it is",
    }
```

```
    # 4. Generate a 256-bit AES key to use with your keyring.
    # In practice, you should get this key from a secure key management system such as
an HSM.

    # Here, the input to secrets.token_bytes() = 32 bytes = 256 bits
    static_key = secrets.token_bytes(32)

    # 5. Create a Raw AES keyring
    # We choose to use a raw AES keyring, but any keyring can be used with streaming.
    mat_prov: AwsCryptographicMaterialProviders = AwsCryptographicMaterialProviders(
        config=MaterialProvidersConfig()
    )

    keyring_input: CreateRawAesKeyringInput = CreateRawAesKeyringInput(
        key_namespace=key_name_space,
        key_name=key_name,
        wrapping_key=static_key,
        wrapping_alg=AesWrappingAlg.ALG_AES256_GCM_IV12_TAG16
    )

    raw_aes_keyring: IKeyring = mat_prov.create_raw_aes_keyring(
        input=keyring_input
    )

    # 6. Encrypt the data stream with the encryptionContext
    with open(plaintext_filename, 'rb') as pt_file, open(ciphertext_filename, 'wb') as
ct_file:
        with client.stream(
            mode='e',
            source=pt_file,
            keyring=raw_aes_keyring,
            encryption_context=encryption_context
        ) as encryptor:
            for chunk in encryptor:
                ct_file.write(chunk)

    # 7. Demonstrate that the ciphertext and plaintext are different.
    # (This is an example for demonstration; you do not need to do this in your own
code.)
    assert not filecmp.cmp(plaintext_filename, ciphertext_filename), \
        "Ciphertext and plaintext data are the same. Invalid encryption"
```

```
    # 8. Decrypt your encrypted data stream using the same keyring you used on
encrypt.
    with open(ciphertext_filename, 'rb') as ct_file, open(decrypted_filename, 'wb') as
pt_file:
        with client.stream(
            mode='d',
            source=ct_file,
            keyring=raw_aes_keyring,
            encryption_context=encryption_context
        ) as decryptor:
            for chunk in decryptor:
                pt_file.write(chunk)

    # 10. Demonstrate that the decrypted plaintext is identical to the original
plaintext.
    # (This is an example for demonstration; you do not need to do this in your own
code.)
    assert filecmp.cmp(plaintext_filename, decrypted_filename), \
        "Decrypted plaintext should be identical to the original plaintext. Invalid
decryption"
```

AWS Encryption SDK untuk Rust

Topik ini menjelaskan cara menginstal dan menggunakan AWS Encryption SDK for Rust. Untuk detail tentang pemrograman dengan AWS Encryption SDK for Rust, lihat direktori Rust dari aws-encryption-sdk repositori di. GitHub

The AWS Encryption SDK for Rust berbeda dari beberapa implementasi bahasa pemrograman lainnya dengan AWS Encryption SDK cara berikut:

- Tidak ada dukungan untuk caching kunci data. Namun, AWS Encryption SDK for Rust mendukung keyring AWS KMS Hierarchical, solusi caching bahan kriptografi alternatif.
- Tidak ada dukungan untuk streaming data

The AWS Encryption SDK for Rust mencakup semua fitur keamanan yang diperkenalkan dalam versi 2.0. x dan yang lebih baru dari implementasi bahasa lain dari. AWS Encryption SDK Namun, jika Anda menggunakan for Rust AWS Encryption SDK untuk mendekripsi data yang dienkripsi oleh pra-2.0. x versi implementasi bahasa lain dari AWS Encryption SDK, Anda mungkin perlu menyesuaikan kebijakan komitmen Anda. Lihat perinciannya di Cara menetapkan kebijakan komitmen Anda.

The AWS Encryption SDK for Rust adalah produk dari AWS Encryption SDK in Dafny, bahasa verifikasi formal di mana Anda menulis spesifikasi, kode untuk mengimplementasikannya, dan bukti untuk mengujinya. Hasilnya adalah perpustakaan yang mengimplementasikan fitur-fitur AWS Encryption SDK dalam kerangka kerja yang menjamin kebenaran fungsional.

Pelajari Lebih Lanjut

- Untuk contoh yang menunjukkan cara mengonfigurasi opsi di AWS Encryption SDK, seperti menentukan rangkaian algoritme alternatif, membatasi kunci data terenkripsi, dan menggunakan kunci AWS KMS Multi-region, lihat. Mengkonfigurasi AWS Encryption SDK
- Untuk contoh yang menunjukkan cara mengonfigurasi dan menggunakan AWS Encryption SDK untuk Rust, lihat contoh Rust di aws-encryption-sdk repositori aktif. GitHub

Topik

Prasyarat

Sebelum Anda menginstal AWS Encryption SDK untuk Rust, pastikan Anda memiliki prasyarat berikut.

Instal Rust dan Cargo

Instal rilis stabil Rust saat ini menggunakan rustup.

Untuk informasi lebih lanjut tentang mengunduh dan menginstal rustup, lihat prosedur instalasi di The Cargo Book.

Penginstalan

The AWS Encryption SDK for Rust tersedia sebagai `aws-esdk`peti di Crates.io. Untuk detail tentang menginstal dan membangun AWS Encryption SDK untuk Rust, lihat README.md di repositori di. aws-encryption-sdk GitHub

Anda dapat menginstal AWS Encryption SDK for Rust dengan cara berikut.

Secara manual

Untuk menginstal AWS Encryption SDK for Rust, kloning atau unduh aws-encryption-sdk GitHub repositori.

Menggunakan Crates.io

Jalankan perintah Cargo berikut di direktori proyek Anda:

```
cargo add aws-esdk
```

Atau tambahkan baris berikut ke Cargo.toml Anda:

```
aws-esdk = "<version>"
```

AWS Encryption SDK untuk kode contoh Rust

Contoh berikut menunjukkan pola pengkodean dasar yang Anda gunakan saat memprogram dengan AWS Encryption SDK for Rust. Secara khusus, Anda membuat instance perpustakaan AWS Encryption SDK dan penyedia materi. Kemudian, sebelum memanggil setiap metode, Anda membuat instance objek yang mendefinisikan input untuk metode tersebut.

Untuk contoh yang menunjukkan cara mengonfigurasi opsi di AWS Encryption SDK, seperti menentukan rangkaian algoritme alternatif dan membatasi kunci data terenkripsi, lihat contoh Rust di repositori aktif. aws-encryption-sdk GitHub

Mengenkripsi dan mendekripsi data di for Rust AWS Encryption SDK

Contoh ini menunjukkan pola dasar untuk mengenkripsi dan mendekripsi data. Ini mengenkripsi file kecil dengan kunci data yang dilindungi oleh satu kunci AWS KMS pembungkus.

Langkah 1: Instantiate. AWS Encryption SDK

Anda akan menggunakan metode dalam AWS Encryption SDK untuk mengenkripsi dan mendekripsi data.

```
let esdk_config = AwsEncryptionSdkConfig::builder().build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;
```

Langkah 2: Buat AWS KMS klien.

```
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);
```

Opsional: Buat konteks enkripsi Anda.

```
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);
```

Langkah 3: Buat instance perpustakaan penyedia materi.

Anda akan menggunakan metode di pustaka penyedia materi untuk membuat keyrings yang menentukan kunci mana yang melindungi data Anda.

```
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;
```

Langkah 4: Buat AWS KMS keyring.

Untuk membuat keyring, panggil metode keyring dengan objek input keyring. Contoh ini menggunakan `create_aws_kms_keyring()` metode dan menentukan satu kunci KMS.

```
let kms_keyring = mpl
    .create_aws_kms_keyring()
    .kms_key_id(kms_key_id)
    .kms_client(kms_client)
    .send()
    .await?;
```

Langkah 5: Enkripsi plaintext.

```
let plaintext = example_data.as_bytes();

let encryption_response = esdk_client.encrypt()
```

```
    .plaintext(plaintext)
    .keyring(kms_keyring.clone())
    .encryption_context(encryption_context.clone())
    .send()
    .await?;

let ciphertext = encryption_response
                    .ciphertext
                    .expect("Unable to unwrap ciphertext from encryption response");
```

Langkah 6: Dekripsi data terenkripsi Anda menggunakan keyring yang sama yang Anda gunakan pada enkripsi.

```
let decryption_response = esdk_client.decrypt()
    .ciphertext(ciphertext)
    .keyring(kms_keyring)
    // Provide the encryption context that was supplied to the encrypt method
    .encryption_context(encryption_context)
    .send()
    .await?;

let decrypted_plaintext = decryption_response
                            .plaintext
                            .expect("Unable to unwrap plaintext from decryption
 response");
```

AWS Encryption SDK antarmuka baris perintah

AWS Encryption SDK Command Line Interface (AWS Encryption CLI) memungkinkan Anda untuk menggunakan AWS Encryption SDK untuk mengenkripsi dan mendekripsi data secara interaktif di baris perintah dan skrip. Anda tidak perlu keahlian kriptografi atau pemrograman.

> **Note**
>
> Versi CLI AWS Enkripsi lebih awal dari 4.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.1. x dan yang lebih baru ke versi terbaru CLI AWS Enkripsi tanpa perubahan kode atau data apa pun. Namun, fitur keamanan baru diperkenalkan di versi 2.1. x tidak kompatibel ke belakang. Untuk memperbarui dari versi 1.7. x atau sebelumnya, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi CLI AWS Enkripsi. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Seperti semua implementasi AWS Encryption SDK, CLI AWS Enkripsi menawarkan fitur perlindungan data tingkat lanjut. Ini termasuk enkripsi amplop, data otentikasi tambahan (AAD), dan rangkaian algoritma kunci simetris yang aman, diautentikasi, seperti AES-GCM 256-bit dengan derivasi kunci, komitmen kunci, dan penandatanganan.

CLI AWS Enkripsi dibangun di atas AWS Encryption SDK for Pythondan didukung di Linux, macOS, dan Windows. Anda dapat menjalankan perintah dan skrip untuk mengenkripsi dan mendekripsi data Anda di shell pilihan Anda di Linux atau macOS, di jendela Command Prompt (cmd.exe) di Windows, dan di konsol di sistem apa pun. PowerShell

Semua implementasi khusus bahasa, termasuk AWS CLI Enkripsi AWS Encryption SDK, dapat dioperasikan secara interoperable. Misalnya, Anda dapat mengenkripsi data dengan AWS Encryption SDK for Javadan mendekripsi dengan CLI Enkripsi AWS .

Topik ini memperkenalkan CLI AWS Enkripsi, menjelaskan cara menginstal dan menggunakannya, dan memberikan beberapa contoh untuk membantu Anda memulai. Untuk memulai dengan cepat, lihat Cara Mengenkripsi dan Mendekripsi Data Anda dengan AWS CLI Enkripsi di Blog Keamanan. AWS Untuk informasi lebih rinci, lihat Baca Dokumen, dan bergabunglah dengan kami dalam mengembangkan CLI AWS Enkripsi di aws-encryption-sdk-clirepositori. GitHub

Performa

CLI AWS Enkripsi dibangun di atas file. AWS Encryption SDK for Python Setiap kali Anda menjalankan CLI, Anda memulai instance baru runtime Python. Untuk meningkatkan kinerja, bila memungkinkan, gunakan satu perintah alih-alih serangkaian perintah independen. Misalnya, jalankan satu perintah yang memproses file dalam direktori secara rekursif alih-alih menjalankan perintah terpisah untuk setiap file.

Topik

- Menginstal antarmuka baris AWS Encryption SDK perintah
- Cara menggunakan CLI AWS Enkripsi
- Contoh CLI AWS Enkripsi

- AWS Encryption SDK Sintaks CLI dan referensi parameter
- Versi CLI AWS Enkripsi

Menginstal antarmuka baris AWS Encryption SDK perintah

Topik ini menjelaskan cara menginstal CLI AWS Enkripsi. Untuk informasi lebih lanjut, lihat aws-encryption-sdk-clirepositori GitHub dan Baca Dokumen.

Topik

- Memasang prasyarat
- Menginstal dan memperbarui CLI AWS Enkripsi

Memasang prasyarat

CLI AWS Enkripsi dibangun di atas file. AWS Encryption SDK for Python Untuk menginstal CLI AWS Enkripsi, Anda memerlukan Python dan, alat manajemen paket `pip` Python. Python dan `pip` tersedia di semua platform yang didukung.

Instal prasyarat berikut sebelum Anda menginstal CLI Enkripsi, AWS

Python

Python 3.8 atau yang lebih baru diperlukan oleh Encryption AWS CLI versi 4.2.0 dan yang lebih baru.

Versi sebelumnya dari AWS Encryption CLI mendukung Python 2.7 dan 3.4 dan yang lebih baru, tetapi kami menyarankan Anda menggunakan versi terbaru dari Encryption CLI. AWS

Python termasuk dalam sebagian besar instalasi Linux dan macOS, tetapi Anda perlu meningkatkan ke Python 3.6 atau yang lebih baru. Kami menyarankan Anda menggunakan versi terbaru Python. Pada Windows, Anda harus menginstal Python; itu tidak diinstal secara default. Untuk mengunduh dan menginstal Python, lihat unduhan Python.

Untuk menentukan apakah Python diinstal, pada baris perintah, ketik berikut ini.

```
python
```

Untuk memeriksa versi Python, gunakan parameter `-V` (huruf besar V).

```
python -V
```

Di Windows, setelah Anda menginstal Python, tambahkan path ke `Python.exe` file ke nilai variabel lingkungan Path.

Secara default, Python dipasang di direktori semua pengguna atau di direktori profil pengguna (`$homeatau%userprofile%`) di subdirektori. `AppData\Local\Programs\Python` Untuk menemukan lokasi `Python.exe` file di sistem Anda, periksa salah satu kunci registri berikut. Anda dapat menggunakan PowerShell untuk mencari registri.

```
PS C:\> dir HKLM:\Software\Python\PythonCore\version\InstallPath
# -or-
PS C:\> dir HKCU:\Software\Python\PythonCore\version\InstallPath
```

pip

`pip`adalah manajer paket Python. Untuk menginstal CLI AWS Enkripsi dan dependensinya, Anda memerlukan `pip` 8.1 atau lebih baru. Untuk bantuan menginstal atau meningkatkan`pip`, lihat Instalasi dalam `pip` dokumentasi.

Pada instalasi Linux, versi `pip` lebih awal dari 8.1 tidak dapat membangun pustaka kriptografi yang dibutuhkan AWS CLI Enkripsi. Jika Anda memilih untuk tidak memperbarui `pip` versi, Anda dapat menginstal alat build secara terpisah. Untuk informasi selengkapnya, lihat Membangun kriptografi di Linux.

AWS Command Line Interface

AWS Command Line Interface (AWS CLI) diperlukan hanya jika Anda menggunakan AWS KMS keys in AWS Key Management Service (AWS KMS) dengan CLI AWS Enkripsi. Jika Anda menggunakan penyedia kunci master yang berbeda, tidak AWS CLI diperlukan.

Untuk menggunakan AWS KMS keys CLI AWS Enkripsi, Anda perlu menginstal dan mengkonfigurasi file. AWS CLI Konfigurasi membuat kredensional yang Anda gunakan untuk mengautentikasi agar AWS KMS tersedia untuk CLI Enkripsi AWS .

Menginstal dan memperbarui CLI AWS Enkripsi

Instal CLI AWS Enkripsi versi terbaru. Ketika Anda menggunakan `pip` untuk menginstal CLI AWS Enkripsi, secara otomatis menginstal pustaka yang dibutuhkan CLI, termasuk, pustaka kriptografi Python, AWS Encryption SDK for Pythondan file. AWS SDK untuk Python (Boto3)

> **Note**
>
> Versi CLI AWS Enkripsi lebih awal dari 4.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.1. x dan yang lebih baru ke versi terbaru CLI AWS Enkripsi tanpa perubahan kode atau data apa pun. Namun, fitur keamanan baru diperkenalkan di versi 2.1. x tidak kompatibel ke belakang. Untuk memperbarui dari versi 1.7. x atau sebelumnya, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi CLI AWS Enkripsi. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.
> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Untuk menginstal versi terbaru dari AWS Encryption CLI

```
pip install aws-encryption-sdk-cli
```

Untuk meng-upgrade ke versi terbaru dari AWS Encryption CLI

```
pip install --upgrade aws-encryption-sdk-cli
```

Untuk menemukan nomor versi CLI AWS Enkripsi Anda dan AWS Encryption SDK

```
aws-encryption-cli --version
```

Output mencantumkan nomor versi kedua pustaka.

```
aws-encryption-sdk-cli/2.1.0 aws-encryption-sdk/2.0.0
```

Untuk meng-upgrade ke versi terbaru dari AWS Encryption CLI

```
pip install --upgrade aws-encryption-sdk-cli
```

Menginstal CLI AWS Enkripsi juga menginstal versi terbaru dari AWS SDK untuk Python (Boto3), jika belum diinstal. Jika Boto3 diinstal, penginstal memverifikasi versi Boto3 dan memperbaruinya jika diperlukan.

Untuk menemukan versi Boto3 yang Anda instal

```
pip show boto3
```

Untuk memperbarui ke versi terbaru Boto3

```
pip install --upgrade boto3
```

Untuk menginstal versi CLI AWS Enkripsi yang saat ini sedang dalam pengembangan, lihat aws-encryption-sdk-clirepositori aktif. GitHub

Untuk detail selengkapnya tentang penggunaan `pip` untuk menginstal dan memutakhirkan paket Python, lihat dokumentasi pip.

Cara menggunakan CLI AWS Enkripsi

Topik ini menjelaskan cara menggunakan parameter dalam CLI AWS Enkripsi. Sebagai contoh, lihat Contoh CLI AWS Enkripsi. Untuk dokumentasi selengkapnya, lihat Membaca Dokumen. Sintaks yang ditunjukkan dalam contoh ini adalah untuk AWS Enkripsi CLI versi 2.1. x dan kemudian.

> **Note**
>
> Versi CLI AWS Enkripsi lebih awal dari 4.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.1. x dan yang lebih baru ke versi terbaru CLI AWS Enkripsi tanpa perubahan kode atau data apa pun. Namun, fitur keamanan baru diperkenalkan di versi 2.1. x tidak kompatibel ke belakang. Untuk memperbarui dari versi 1.7. x atau sebelumnya, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi CLI AWS Enkripsi. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.
> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Untuk contoh yang menunjukkan cara menggunakan fitur keamanan yang membatasi kunci data terenkripsi, lihat. Membatasi kunci data terenkripsi

Untuk contoh yang menunjukkan cara menggunakan kunci AWS KMS Multi-region, lihatMenggunakan Multi-region AWS KMS keys.

Topik

- Cara mengenkripsi dan mendekripsi data
- Cara menentukan kunci pembungkus
- Cara memberikan masukan
- Cara menentukan lokasi output
- Cara menggunakan konteks enkripsi
- Cara menentukan kebijakan komitmen
- Cara menyimpan parameter dalam file konfigurasi

Cara mengenkripsi dan mendekripsi data

AWS Enkripsi CLI menggunakan fitur AWS Encryption SDK untuk membuatnya mudah untuk mengenkripsi dan mendekripsi data dengan aman.

> **Note**
>
> `--master-keys`Parameter tidak digunakan lagi di versi 1.8. x dari CLI AWS Enkripsi dan dihapus dalam versi 2.1. x. Sebagai gantinya, gunakan `--wrapping-keys` parameternya. Dimulai pada versi 2.1. x, `--wrapping-keys` parameter diperlukan saat mengenkripsi dan mendekripsi. Lihat perinciannya di AWS Encryption SDK Sintaks CLI dan referensi parameter.

- Saat Anda mengenkripsi data di CLI AWS Enkripsi, Anda menentukan data teks biasa dan kunci pembungkus (atau kunci master), seperti in (). AWS KMS key AWS Key Management Service AWS KMS Jika Anda menggunakan penyedia kunci master kustom, Anda juga perlu menentukan penyedia. Anda juga menentukan lokasi keluaran untuk pesan terenkripsi dan untuk metadata tentang operasi enkripsi. Konteks enkripsi bersifat opsional, tetapi disarankan.

  Dalam versi 1.8. x, `--commitment-policy` parameter diperlukan saat Anda menggunakan `--wrapping-keys` parameter; jika tidak maka tidak valid. Dimulai pada versi 2.1. x, `--commitment-policy` parameternya opsional, tetapi disarankan.

```
aws-encryption-cli --encrypt --input myPlaintextData \
                   --wrapping-keys key=1234abcd-12ab-34cd-56ef-1234567890ab \
                   --output myEncryptedMessage \
                   --metadata-output ~/metadata \
                   --encryption-context purpose=test \
                   --commitment-policy require-encrypt-require-decrypt
```

CLI AWS Enkripsi mengenkripsi data Anda di bawah kunci data unik. Kemudian mengenkripsi kunci data di bawah kunci pembungkus yang Anda tentukan. Ia mengembalikan pesan terenkripsi dan metadata tentang operasi. Pesan terenkripsi berisi data terenkripsi Anda (ciphertext) dan salinan kunci data terenkripsi. Anda tidak perlu khawatir tentang menyimpan, mengelola, atau kehilangan kunci data.

- Ketika Anda mendekripsi data, Anda meneruskan pesan terenkripsi Anda, konteks enkripsi opsional, dan lokasi untuk output plaintext dan metadata. Anda juga menentukan kunci pembungkus yang dapat digunakan CLI AWS Enkripsi untuk mendekripsi pesan, atau memberi tahu CLI AWS Enkripsi bahwa ia dapat menggunakan kunci pembungkus apa pun yang mengenkripsi pesan.

  Dimulai pada versi 1.8. x, `--wrapping-keys` parameternya opsional saat mendekripsi, tetapi disarankan. Dimulai pada versi 2.1. x, `--wrapping-keys` parameter diperlukan saat mengenkripsi dan mendekripsi.

  Saat mendekripsi, Anda dapat menggunakan atribut kunci `--wrapping-keys` parameter untuk menentukan kunci pembungkus yang mendekripsi data Anda. Menentukan kunci AWS KMS pembungkus saat mendekripsi adalah opsional, tetapi ini adalah praktik terbaik yang mencegah Anda menggunakan kunci yang tidak ingin Anda gunakan. Jika Anda menggunakan penyedia kunci master kustom, Anda harus menentukan penyedia dan kunci pembungkus.

  Jika Anda tidak menggunakan atribut kunci, Anda harus menyetel atribut penemuan `--wrapping-keys` parameter `ketrue`, yang memungkinkan CLI AWS Enkripsi mendekripsi menggunakan kunci pembungkus apa pun yang mengenkripsi pesan.

  Sebagai praktik terbaik, gunakan `--max-encrypted-data-keys` parameter untuk menghindari dekripsi pesan yang salah dengan jumlah kunci data terenkripsi yang berlebihan. Tentukan jumlah yang diharapkan dari kunci data terenkripsi (satu untuk setiap kunci pembungkus yang digunakan

dalam enkripsi) atau maksimum yang wajar (seperti 5). Lihat perinciannya di Membatasi kunci data terenkripsi.

`--buffer`Parameter mengembalikan plaintext hanya setelah semua input diproses, termasuk memverifikasi tanda tangan digital jika ada.

`--decrypt-unsigned`Parameter mendekripsi ciphertext dan memastikan bahwa pesan tidak ditandatangani sebelum dekripsi. Gunakan parameter ini jika Anda menggunakan `--algorithm` parameter dan memilih rangkaian algoritme tanpa penandatanganan digital untuk mengenkripsi data. Jika ciphertext ditandatangani, dekripsi gagal.

Anda dapat menggunakan `--decrypt` atau `--decrypt-unsigned` untuk dekripsi tetapi tidak keduanya.

```
aws-encryption-cli --decrypt --input myEncryptedMessage \
                   --wrapping-keys key=1234abcd-12ab-34cd-56ef-1234567890ab \
                   --output myPlaintextData \
                   --metadata-output ~/metadata \
                   --max-encrypted-data-keys 1 \
                   --buffer \
                   --encryption-context purpose=test \
                   --commitment-policy require-encrypt-require-decrypt
```

CLI AWS Enkripsi menggunakan kunci pembungkus untuk mendekripsi kunci data dalam pesan terenkripsi. Kemudian menggunakan kunci data untuk mendekripsi data Anda. Ini mengembalikan data plaintext dan metadata Anda tentang operasi.

Cara menentukan kunci pembungkus

Saat Anda mengenkripsi data di CLI AWS Enkripsi, Anda perlu menentukan setidaknya satu kunci pembungkus (atau kunci master). Anda dapat menggunakan AWS KMS keys in AWS Key Management Service (AWS KMS), kunci pembungkus dari penyedia kunci master kustom, atau keduanya. Penyedia kunci master kustom dapat berupa penyedia kunci master Python yang kompatibel.

Untuk menentukan kunci pembungkus di versi 1.8. x dan kemudian, gunakan `--wrapping-keys` parameter (`-w`). Nilai parameter ini adalah kumpulan atribut dengan `attribute=value` format. Atribut yang Anda gunakan bergantung pada penyedia kunci master dan perintah.

- AWS KMS. Dalam perintah enkripsi, Anda harus menentukan `--wrapping-keys` parameter dengan atribut kunci. Dimulai pada versi 2.1. x, `--wrapping-keys` parameter juga diperlukan dalam perintah dekripsi. Saat mendekripsi, `--wrapping-keys` parameter harus memiliki atribut kunci atau atribut penemuan dengan nilai `true` (tetapi tidak keduanya). Atribut lainnya adalah opsional.
- Penyedia kunci master kustom. Anda harus menentukan `--wrapping-keys` parameter di setiap perintah. Nilai parameter harus memiliki atribut kunci dan penyedia.

Anda dapat menyertakan beberapa `--wrapping-keys` parameter dan beberapa atribut kunci dalam perintah yang sama.

Membungkus atribut parameter kunci

Nilai `--wrapping-keys` parameter terdiri dari atribut berikut dan nilainya. `--wrapping-keys`Parameter (atau `--master-keys` parameter) diperlukan di semua perintah enkripsi. Dimulai pada versi 2.1. x, `--wrapping-keys` parameter juga diperlukan saat mendekripsi.

Jika nama atau nilai atribut menyertakan spasi atau karakter khusus, lampirkan nama dan nilai dalam tanda kutip. Misalnya, `--wrapping-keys key=12345 "provider=my cool provider"`.

Kunci: Tentukan kunci pembungkus

Gunakan atribut kunci untuk mengidentifikasi kunci pembungkus. Saat mengenkripsi, nilainya dapat berupa pengidentifikasi kunci apa pun yang dikenali oleh penyedia kunci utama.

```
--wrapping-keys key=1234abcd-12ab-34cd-56ef-1234567890ab
```

Dalam perintah enkripsi, Anda harus menyertakan setidaknya satu atribut kunci dan nilai. Untuk mengenkripsi kunci data Anda di bawah beberapa kunci pembungkus, gunakan beberapa atribut kunci.

```
aws-encryption-cli --encrypt --wrapping-keys
 key=1234abcd-12ab-34cd-56ef-1234567890ab key=1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d
```

Dalam perintah enkripsi yang digunakan AWS KMS keys, nilai kunci dapat berupa ID kunci, ARN kuncinya, nama alias, atau alias ARN. Misalnya, perintah enkripsi ini menggunakan alias ARN dalam nilai atribut kunci. Untuk detail tentang pengidentifikasi kunci AWS KMS key, lihat Pengidentifikasi Kunci di Panduan AWS Key Management Service Pengembang.

```
aws-encryption-cli --encrypt --wrapping-keys key=arn:aws:kms:us-
west-2:111122223333:alias/ExampleAlias
```

Dalam perintah dekripsi yang menggunakan penyedia kunci master kustom, atribut kunci dan penyedia diperlukan.

```
\\ Custom master key provider
aws-encryption-cli --decrypt --wrapping-keys provider='myProvider' key='100101'
```

Dalam perintah dekripsi yang digunakan AWS KMS, Anda dapat menggunakan atribut kunci untuk menentukan yang akan digunakan AWS KMS keys untuk mendekripsi, atau atribut penemuan dengan nilai`true`, yang memungkinkan AWS CLI Enkripsi menggunakan apa pun AWS KMS key yang digunakan untuk mengenkripsi pesan. Jika Anda menentukan AWS KMS key, itu harus menjadi salah satu kunci pembungkus yang digunakan untuk mengenkripsi pesan.

Menentukan kunci pembungkus adalah praktik AWS Encryption SDK terbaik. Ini memastikan bahwa Anda menggunakan yang ingin AWS KMS key Anda gunakan.

Dalam perintah dekripsi, nilai atribut kunci harus berupa ARN kunci.

```
\\ AWS KMS key
aws-encryption-cli --decrypt --wrapping-keys key=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Penemuan: Gunakan apa saja AWS KMS key saat mendekripsi

Jika Anda tidak perlu membatasi penggunaan saat mendekripsi, Anda dapat menggunakan atribut penemuan dengan nilai. AWS KMS keys `true` Nilai `true` memungkinkan CLI AWS Enkripsi untuk mendekripsi menggunakan apa pun AWS KMS key yang mengenkripsi pesan. Jika Anda tidak menentukan atribut penemuan, penemuan adalah `false` (default). Atribut penemuan hanya valid dalam perintah dekripsi dan hanya ketika pesan dienkripsi dengan. AWS KMS keys

Atribut penemuan dengan nilai `true` adalah alternatif untuk menggunakan atribut kunci untuk menentukan AWS KMS keys. Saat mendekripsi pesan yang dienkripsi AWS KMS keys, setiap `--wrapping-keys` parameter harus memiliki atribut kunci atau atribut penemuan dengan nilai`true`, tetapi tidak keduanya.

Ketika penemuan benar, sebaiknya gunakan atribut partisi penemuan dan akun penemuan untuk membatasi yang AWS KMS keys digunakan pada atribut yang Anda tentukan. Akun AWS Dalam

contoh berikut, atribut penemuan memungkinkan CLI AWS Enkripsi untuk menggunakan apa pun AWS KMS key dalam yang ditentukan. Akun AWS

```
aws-encryption-cli --decrypt --wrapping-keys \
    discovery=true \
    discovery-partition=aws \
    discovery-account=111122223333 \
    discovery-account=444455556666
```

Penyedia: Tentukan penyedia kunci utama

Atribut provider mengidentifikasi penyedia kunci master. Nilai default adalah`aws-kms`, yang mewakili AWS KMS. Jika Anda menggunakan penyedia kunci master yang berbeda, atribut penyedia diperlukan.

```
--wrapping-keys key=12345 provider=my_custom_provider
```

Untuk informasi selengkapnya tentang penggunaan penyedia kunci master kustom (non-#-AWS KMS), lihat topik Konfigurasi Lanjutan dalam file README untuk repositori CLI AWS Enkripsi.

Wilayah: Tentukan Wilayah AWS

Gunakan atribut region untuk menentukan Wilayah AWS dari AWS KMS key. Atribut ini hanya valid dalam perintah enkripsi dan hanya ketika penyedia kunci master. AWS KMS

```
--encrypt --wrapping-keys key=alias/primary-key region=us-east-2
```

AWS Enkripsi perintah CLI menggunakan Wilayah AWS yang ditentukan dalam nilai atribut kunci jika termasuk wilayah, seperti ARN. jika nilai kunci menentukan Wilayah AWS, atribut region diabaikan.

Atribut region lebih diutamakan daripada spesifikasi wilayah lainnya. Jika Anda tidak menggunakan atribut region, perintah AWS Encryption CLI menggunakan yang Wilayah AWS ditentukan dalam profil AWS CLI bernama Anda, jika ada, atau profil default Anda.

Profil: Tentukan profil bernama

Gunakan atribut profil untuk menentukan profil AWS CLI bernama. Profil bernama dapat mencakup kredensil dan file. Wilayah AWS Atribut ini hanya valid jika penyedia kunci master AWS KMS.

```
--wrapping-keys key=alias/primary-key profile=admin-1
```

Anda dapat menggunakan atribut profil untuk menentukan kredensi alternatif dalam perintah enkripsi dan dekripsi. Dalam perintah enkripsi, CLI AWS Enkripsi menggunakan Wilayah AWS dalam profil bernama hanya ketika nilai kunci tidak menyertakan wilayah dan tidak ada atribut wilayah. Dalam perintah dekripsi, profil Wilayah AWS dalam nama diabaikan.

Cara menentukan beberapa tombol pembungkus

Anda dapat menentukan beberapa tombol pembungkus (atau kunci master) di setiap perintah.

Jika Anda menentukan lebih dari satu kunci pembungkus, kunci pembungkus pertama menghasilkan dan mengenkripsi kunci data yang digunakan untuk mengenkripsi data Anda. Kunci pembungkus lainnya mengenkripsi kunci data yang sama. Pesan terenkripsi yang dihasilkan berisi data terenkripsi ("ciphertext") dan kumpulan kunci data terenkripsi, satu dienkripsi oleh setiap kunci pembungkus. Setiap pembungkus dapat mendekripsi satu kunci data terenkripsi dan kemudian mendekripsi data.

Ada dua cara untuk menentukan beberapa kunci pembungkus:

- Sertakan beberapa atribut kunci dalam nilai `--wrapping-keys` parameter.

```
$key_oregon=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
$key_ohio=arn:aws:kms:us-east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef

--wrapping-keys key=$key_oregon key=$key_ohio
```

- Sertakan beberapa `--wrapping-keys` parameter dalam perintah yang sama. Gunakan sintaks ini ketika nilai atribut yang Anda tentukan tidak berlaku untuk semua kunci pembungkus dalam perintah.

```
--wrapping-keys region=us-east-2 key=alias/test_key \
--wrapping-keys region=us-west-1 key=alias/test_key
```

Atribut penemuan dengan nilai `true` memungkinkan CLI AWS Enkripsi menggunakan apa pun AWS KMS key yang mengenkripsi pesan. Jika Anda menggunakan beberapa `--wrapping-keys` parameter dalam perintah yang sama, menggunakan `discovery=true` `--wrapping-`

`keys` parameter apa pun secara efektif mengesampingkan batas atribut kunci di parameter lain`--wrapping-keys`.

Misalnya, dalam perintah berikut, atribut kunci dalam `--wrapping-keys` parameter pertama membatasi CLI AWS Enkripsi ke yang ditentukan. AWS KMS key Namun, atribut penemuan di `--wrapping-keys` parameter kedua memungkinkan CLI AWS Enkripsi menggunakan apa pun AWS KMS key di akun yang ditentukan untuk mendekripsi pesan.

```
aws-encryption-cli --decrypt \
    --wrapping-keys key=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --wrapping-keys discovery=true \
                    discovery-partition=aws \
                    discovery-account=111122223333 \
                    discovery-account=444455556666
```

Cara memberikan masukan

Operasi enkripsi di CLI AWS Enkripsi mengambil data teks biasa sebagai input dan mengembalikan pesan terenkripsi. Operasi dekripsi mengambil pesan terenkripsi sebagai input dan mengembalikan data plaintext.

`--input`Parameter (`-i`), yang memberi tahu AWS Encryption CLI di mana menemukan input, diperlukan di semua perintah Encryption AWS CLI.

Anda dapat memberikan masukan dengan salah satu cara berikut:

- Gunakan file.

  ```
  --input myData.txt
  ```

- Gunakan pola nama file.

  ```
  --input testdir/*.xml
  ```

- Gunakan pola nama direktori atau direktori. Ketika input adalah direktori, `--recursive` parameter (`-r`,`-R`) diperlukan.

  ```
  --input testdir --recursive
  ```

- Input pipa ke perintah (stdin). Gunakan nilai `-` untuk `--input` parameter. (`--input`Parameter selalu diperlukan.)

```
echo 'Hello World' | aws-encryption-cli --encrypt --input -
```

Cara menentukan lokasi output

`--output`Parameter memberi tahu CLI AWS Enkripsi tempat menulis hasil operasi enkripsi atau dekripsi. Hal ini diperlukan dalam setiap perintah AWS Enkripsi CLI. CLI AWS Enkripsi membuat file output baru untuk setiap file input dalam operasi.

Jika file keluaran sudah ada, secara default, CLI AWS Enkripsi mencetak peringatan, lalu menimpa file tersebut. Untuk mencegah penimpaan, gunakan `--interactive` parameter, yang meminta Anda untuk konfirmasi sebelum menimpa, atau`--no-overwrite`, yang melewatkan input jika output akan menyebabkan penimpaan. Untuk menekan peringatan penimpaan, gunakan. `--quiet` Untuk menangkap kesalahan dan peringatan dari CLI AWS Enkripsi, gunakan operator `2>&1` pengalihan untuk menuliskannya ke aliran output.

> **Note**
>
> Perintah yang menimpa file output dimulai dengan menghapus file output. Jika perintah gagal, file output mungkin sudah dihapus.

Anda dapat lokasi output dalam beberapa cara.

- Tentukan nama file. Jika Anda menentukan jalur ke file, semua direktori di jalur harus ada sebelum perintah berjalan.

```
--output myEncryptedData.txt
```

- Tentukan direktori. Direktori output harus ada sebelum perintah berjalan.

  Jika input berisi subdirektori, perintah mereproduksi subdirektori di bawah direktori yang ditentukan.

```
--output Test
```

Ketika lokasi output adalah direktori (tanpa nama file), CLI AWS Enkripsi membuat nama file output berdasarkan nama file input ditambah akhiran. Enkripsi operasi append `.encrypted` ke nama file input dan operasi dekripsi ditambahkan. `.decrypted` Untuk mengubah sufiks, gunakan `--suffix` parameter.

Misalnya, jika Anda mengenkripsi`file.txt`, perintah enkripsi dibuat. `file.txt.encrypted` Jika Anda mendekripsi`file.txt.encrypted`, perintah dekripsi akan dibuat. `file.txt.encrypted.decrypted`

- Tulis ke baris perintah (stdout). Masukkan nilai `-` untuk `--output` parameter. Anda dapat menggunakan `--output -` untuk menyalurkan output ke perintah atau program lain.

```
--output -
```

Cara menggunakan konteks enkripsi

AWS Enkripsi CLI memungkinkan Anda menyediakan konteks enkripsi dalam mengenkripsi dan mendekripsi perintah. Ini tidak diperlukan, tetapi ini adalah praktik terbaik kriptografi yang kami rekomendasikan.

Konteks enkripsi adalah jenis data otentikasi tambahan yang sewenang-wenang dan non-rahasia. Dalam CLI AWS Enkripsi, konteks enkripsi terdiri dari kumpulan pasangan. `name=value` Anda dapat menggunakan konten apa pun dalam pasangan, termasuk informasi tentang file, data yang membantu Anda menemukan operasi enkripsi di log, atau data yang diperlukan oleh hibah atau kebijakan Anda.

Dalam perintah enkripsi

Konteks enkripsi yang Anda tentukan dalam perintah enkripsi, bersama dengan pasangan tambahan apa pun yang ditambahkan CMM, terikat secara kriptografis ke data terenkripsi. Ini juga termasuk (dalam teks biasa) dalam pesan terenkripsi yang dikembalikan oleh perintah. Jika Anda menggunakan AWS KMS key, konteks enkripsi juga mungkin muncul dalam teks biasa dalam catatan audit dan log, seperti. AWS CloudTrail

Contoh berikut menunjukkan konteks enkripsi dengan tiga `name=value` pasang.

```
--encryption-context purpose=test dept=IT class=confidential
```

Dalam perintah dekripsi

Dalam perintah dekripsi, konteks enkripsi membantu Anda mengonfirmasi bahwa Anda mendekripsi pesan terenkripsi yang tepat.

Anda tidak diharuskan untuk menyediakan konteks enkripsi dalam perintah dekripsi, bahkan jika konteks enkripsi digunakan pada enkripsi. Namun, jika Anda melakukannya, CLI AWS Enkripsi memverifikasi bahwa setiap elemen dalam konteks enkripsi perintah dekripsi cocok dengan elemen dalam konteks enkripsi pesan terenkripsi. Jika ada elemen yang tidak cocok, perintah dekripsi gagal.

Misalnya, perintah berikut mendekripsi pesan terenkripsi hanya jika konteks enkripsi termasuk. `dept=IT`

```
aws-encryption-cli --decrypt --encryption-context dept=IT ...
```

Konteks enkripsi adalah bagian penting dari strategi keamanan Anda. Namun, ketika memilih konteks enkripsi, ingatlah bahwa nilainya bukan rahasia. Jangan sertakan data rahasia apa pun dalam konteks enkripsi.

Untuk menentukan konteks enkripsi

- Dalam perintah enkripsi, gunakan `--encryption-context` parameter dengan satu atau lebih `name=value` pasangan. Gunakan spasi untuk memisahkan setiap pasangan.

  ```
  --encryption-context name=value [name=value] ...
  ```

- Dalam perintah dekripsi, nilai `--encryption-context` parameter dapat mencakup `name=value` pasangan, `name` elemen (tanpa nilai), atau kombinasi keduanya.

  ```
  --encryption-context name[=value] [name] [name=value] ...
  ```

Jika `name` atau `value` dalam `name=value` pasangan menyertakan spasi atau karakter khusus, lampirkan seluruh pasangan dalam tanda kutip.

```
--encryption-context "department=software engineering" "Wilayah AWS=us-west-2"
```

Misalnya, perintah enkripsi ini mencakup konteks enkripsi dengan dua pasang, `purpose=test` dan`dept=23`.

```
aws-encryption-cli --encrypt --encryption-context purpose=test dept=23 ...
```

Perintah dekripsi ini akan berhasil. Konteks enkripsi dalam setiap perintah adalah bagian dari konteks enkripsi asli.

```
\\ Any one or both of the encryption context pairs
aws-encryption-cli --decrypt --encryption-context dept=23 ...

\\ Any one or both of the encryption context names
aws-encryption-cli --decrypt --encryption-context purpose ...

\\ Any combination of names and pairs
aws-encryption-cli --decrypt --encryption-context dept purpose=test ...
```

Namun, perintah dekripsi ini akan gagal. Konteks enkripsi dalam pesan terenkripsi tidak mengandung elemen yang ditentukan.

```
aws-encryption-cli --decrypt --encryption-context dept=Finance ...
aws-encryption-cli --decrypt --encryption-context scope ...
```

Cara menentukan kebijakan komitmen

Untuk menetapkan kebijakan komitmen untuk perintah, gunakan `--commitment-policy`parameter. Parameter ini diperkenalkan dalam versi 1.8. x. Ini berlaku dalam perintah enkripsi dan dekripsi. Kebijakan komitmen yang Anda tetapkan hanya berlaku untuk perintah yang muncul. Jika Anda tidak menetapkan kebijakan komitmen untuk suatu perintah, CLI AWS Enkripsi menggunakan nilai default.

Misalnya, nilai parameter berikut menetapkan kebijakan komitmen`require-encrypt-allow-decrypt`, yang selalu mengenkripsi dengan komitmen utama, tetapi akan mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen utama.

```
--commitment-policy require-encrypt-allow-decrypt
```

Cara menyimpan parameter dalam file konfigurasi

Anda dapat menghemat waktu dan menghindari kesalahan pengetikan dengan menyimpan parameter dan nilai CLI AWS Enkripsi yang sering digunakan dalam file konfigurasi.

File konfigurasi adalah file teks yang berisi parameter dan nilai untuk perintah CLI AWS Enkripsi. Ketika Anda merujuk ke file konfigurasi dalam perintah AWS Encryption CLI, referensi digantikan oleh parameter dan nilai dalam file konfigurasi. Efeknya sama adalah jika Anda mengetik konten file di baris perintah. File konfigurasi dapat memiliki nama apa pun dan dapat ditemukan di direktori mana pun yang dapat diakses pengguna saat ini.

Contoh file konfigurasi berikut,`key.conf`, menentukan dua AWS KMS keys di Wilayah yang berbeda.

```
--wrapping-keys key=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
--wrapping-keys key=arn:aws:kms:us-
east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef
```

Untuk menggunakan file konfigurasi dalam perintah, awali nama file dengan tanda at (@). Di PowerShell konsol, gunakan karakter backtick untuk keluar dari tanda at (`@).

Perintah contoh ini menggunakan `key.conf` file dalam perintah enkripsi.

Bash

```
$ aws-encryption-cli -e @key.conf -i hello.txt -o testdir
```

PowerShell

```
PS C:\> aws-encryption-cli -e `@key.conf -i .\Hello.txt -o .\TestDir
```

Aturan file konfigurasi

Aturan untuk menggunakan file konfigurasi adalah sebagai berikut:

- Anda dapat menyertakan beberapa parameter di setiap file konfigurasi dan mencantumkannya dalam urutan apa pun. Buat daftar setiap parameter dengan nilainya (jika ada) pada baris terpisah.
- Gunakan # untuk menambahkan komentar ke semua atau sebagian baris.
- Anda dapat menyertakan referensi ke file konfigurasi lainnya. Jangan gunakan backtick untuk menghindari @ tanda, bahkan masuk PowerShell.
- Jika Anda menggunakan tanda kutip dalam file konfigurasi, teks yang dikutip tidak dapat menjangkau beberapa baris.

Misalnya, ini adalah isi dari `encrypt.conf` file contoh.

```
# Archive Files
--encrypt
--output /archive/logs
--recursive
--interactive
--encryption-context class=unclassified dept=IT
--suffix  # No suffix
--metadata-output ~/metadata
@caching.conf  # Use limited caching
```

Anda juga dapat menyertakan beberapa file konfigurasi dalam sebuah perintah. Perintah contoh ini menggunakan file `encrypt.conf` dan `master-keys.conf` konfigurasi.

Bash

```
$  aws-encryption-cli -i /usr/logs @encrypt.conf @master-keys.conf
```

PowerShell

```
PS C:\> aws-encryption-cli -i $home\Test\*.log `@encrypt.conf `@master-keys.conf
```

Berikutnya: Coba contoh AWS Encryption CLI

Contoh CLI AWS Enkripsi

Gunakan contoh berikut untuk mencoba CLI AWS Enkripsi pada platform yang Anda inginkan. Untuk bantuan dengan kunci master dan parameter lainnya, lihatCara menggunakan CLI AWS Enkripsi. Untuk referensi cepat, lihatAWS Encryption SDK Sintaks CLI dan referensi parameter.

> **Note**
>
> Contoh berikut menggunakan sintaks untuk AWS Enkripsi CLI versi 2.1. x.
> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Untuk contoh yang menunjukkan cara menggunakan fitur keamanan yang membatasi kunci data terenkripsi, lihat. Membatasi kunci data terenkripsi

Untuk contoh yang menunjukkan cara menggunakan kunci AWS KMS Multi-region, lihatMenggunakan Multi-region AWS KMS keys.

Topik

- Mengenkripsi file
- Mendekripsi file
- Mengenkripsi semua file dalam direktori
- Mendekripsi semua file dalam direktori
- Mengenkripsi dan mendekripsi pada baris perintah
- Menggunakan beberapa kunci master
- Mengenkripsi dan mendekripsi dalam skrip
- Menggunakan caching kunci data

Mengenkripsi file

Contoh ini menggunakan CLI AWS Enkripsi untuk mengenkripsi isi `hello.txt` file, yang berisi string “Hello World”.

Ketika Anda menjalankan perintah enkripsi pada file, CLI AWS Enkripsi mendapatkan konten file, menghasilkan kunci data unik, mengenkripsi konten file di bawah kunci data, dan kemudian menulis pesan terenkripsi ke file baru.

Perintah pertama menyimpan ARN kunci dari AWS KMS key variabel. `$keyArn` Saat mengenkripsi dengan AWS KMS key, Anda dapat mengidentifikasinya dengan menggunakan ID kunci, ARN kunci, nama alias, atau alias ARN. Untuk detail tentang pengidentifikasi kunci AWS KMS key, lihat Pengidentifikasi Kunci di Panduan AWS Key Management Service Pengembang.

Perintah kedua mengenkripsi isi file. Perintah menggunakan `--encrypt` parameter untuk menentukan operasi dan `--input` parameter untuk menunjukkan file yang akan dienkripsi. `--wrapping-keys`Parameter, dan atribut kunci yang diperlukan, beri tahu perintah untuk menggunakan yang AWS KMS key diwakili oleh kunci ARN.

Perintah menggunakan `--metadata-output` parameter untuk menentukan file teks untuk metadata tentang operasi enkripsi. Sebagai praktik terbaik, perintah menggunakan `--encryption-context` parameter untuk menentukan konteks enkripsi.

Perintah ini juga menggunakan `--commitment-policy`parameter untuk menetapkan kebijakan komitmen secara eksplisit. Dalam versi 1.8. x, parameter ini diperlukan saat Anda menggunakan `--wrapping-keys` parameter. Dimulai pada versi 2.1. x, `--commitment-policy` parameternya opsional, tetapi disarankan.

Nilai `--output` parameter, titik (.), memberi tahu perintah untuk menulis file output ke direktori saat ini.

Bash

```
\\ To run this example, replace the fictitious key ARN with a valid value.
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --wrapping-keys key=$keyArn \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --commitment-policy require-encrypt-require-decrypt \
                     --output .
```

PowerShell

```
# To run this example, replace the fictitious key ARN with a valid value.
PS C:\> $keyArn = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

PS C:\> aws-encryption-cli --encrypt `
                           --input Hello.txt `
                           --wrapping-keys key=$keyArn `
                           --metadata-output $home\Metadata.txt `
                           --commitment-policy require-encrypt-require-decrypt `
                           --encryption-context purpose=test `
                           --output .
```

Ketika perintah enkripsi berhasil, itu tidak mengembalikan output apa pun. Untuk menentukan apakah perintah berhasil, periksa nilai Boolean dalam variabel. $? Ketika perintah berhasil, nilai dari $?

adalah `0` (Bash) atau `True` (PowerShell). Ketika perintah gagal, nilai `$?` adalah bukan nol (Bash) atau `False` (PowerShell).

Bash

```
$ echo $?
0
```

PowerShell

```
PS C:\> $?
True
```

Anda juga dapat menggunakan perintah daftar direktori untuk melihat bahwa perintah enkripsi membuat file baru,`hello.txt.encrypted`. Karena perintah enkripsi tidak menentukan nama file untuk output, CLI AWS Enkripsi menulis output ke file dengan nama yang sama dengan file input ditambah `.encrypted` akhiran. Untuk menggunakan akhiran yang berbeda, atau menekan sufiks, gunakan parameter. `--suffix`

`hello.txt.encrypted`File berisi pesan terenkripsi yang mencakup ciphertext `hello.txt` file, salinan kunci data terenkripsi, dan metadata tambahan, termasuk konteks enkripsi.

Bash

```
$  ls
hello.txt  hello.txt.encrypted
```

PowerShell

```
PS C:\> dir

    Directory: C:\TestCLI

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/15/2017   5:57 PM             11 Hello.txt
-a----        9/17/2017   1:06 PM            585 Hello.txt.encrypted
```

Mendekripsi file

Contoh ini menggunakan CLI AWS Enkripsi untuk mendekripsi isi `Hello.txt.encrypted` file yang dienkripsi pada contoh sebelumnya.

Perintah dekripsi menggunakan `--decrypt` parameter untuk menunjukkan operasi dan `--input` parameter untuk mengidentifikasi file yang akan didekripsi. Nilai `--output` parameter adalah titik yang mewakili direktori saat ini.

`--wrapping-keys`Parameter dengan atribut kunci menentukan kunci pembungkus yang digunakan untuk mendekripsi pesan terenkripsi. Dalam dekripsi perintah dengan AWS KMS keys, nilai atribut kunci harus berupa ARN kunci. `--wrapping-keys`Parameter diperlukan dalam perintah dekripsi. Jika Anda menggunakan AWS KMS keys, Anda dapat menggunakan atribut kunci untuk menentukan AWS KMS keys untuk mendekripsi atau atribut penemuan dengan nilai `true` (tetapi tidak keduanya). Jika Anda menggunakan penyedia kunci master kustom, atribut kunci dan penyedia diperlukan.

`--commitment-policy`Parameternya opsional dimulai pada versi 2.1. x, tetapi disarankan. Menggunakannya secara eksplisit membuat maksud Anda jelas, bahkan jika Anda menentukan nilai default,. `require-encrypt-require-decrypt`

`--encryption-context`Parameter ini opsional dalam perintah dekripsi, bahkan ketika konteks enkripsi disediakan dalam perintah enkripsi. Dalam hal ini, perintah dekripsi menggunakan konteks enkripsi yang sama yang disediakan dalam perintah enkripsi. Sebelum mendekripsi, AWS CLI Enkripsi memverifikasi bahwa konteks enkripsi dalam pesan terenkripsi menyertakan pasangan. `purpose=test` Jika tidak, perintah dekripsi gagal.

`--metadata-output`Parameter menentukan file untuk metadata tentang operasi dekripsi. Nilai `--output` parameter, titik (.), menulis file output ke direktori saat ini.

Sebagai praktik terbaik, gunakan `--max-encrypted-data-keys` parameter untuk menghindari dekripsi pesan yang salah dengan jumlah kunci data terenkripsi yang berlebihan. Tentukan jumlah yang diharapkan dari kunci data terenkripsi (satu untuk setiap kunci pembungkus yang digunakan dalam enkripsi) atau maksimum yang wajar (seperti 5). Lihat perinciannya di Membatasi kunci data terenkripsi.

Plaintext `--buffer` mengembalikan hanya setelah semua input diproses, termasuk memverifikasi tanda tangan digital jika ada.

Bash

```
\\ To run this example, replace the fictitious key ARN with a valid value.
```

```
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys key=$keyArn \
                     --commitment-policy require-encrypt-require-decrypt \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --max-encrypted-data-keys 1 \
                     --buffer \
                     --output .
```

PowerShell

```
\\ To run this example, replace the fictitious key ARN with a valid value.
PS C:\> $keyArn = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

PS C:\> aws-encryption-cli --decrypt `
                           --input Hello.txt.encrypted `
                           --wrapping-keys key=$keyArn `
                           --commitment-policy require-encrypt-require-decrypt `
                           --encryption-context purpose=test `
                           --metadata-output $home\Metadata.txt `
                           --max-encrypted-data-keys 1 `
                           --buffer `
                           --output .
```

Ketika perintah dekripsi berhasil, itu tidak mengembalikan output apa pun. Untuk menentukan apakah perintah berhasil, dapatkan nilai `$?` variabel. Anda juga dapat menggunakan perintah daftar direktori untuk melihat bahwa perintah tersebut membuat file baru dengan `.decrypted` akhiran. Untuk melihat konten plaintext, gunakan perintah untuk mendapatkan konten file, seperti `cat` atau Get-Content.

Bash

```
$  ls
hello.txt  hello.txt.encrypted  hello.txt.encrypted.decrypted

$  cat hello.txt.encrypted.decrypted
Hello World
```

PowerShell

```
PS C:\> dir

    Directory: C:\TestCLI

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/17/2017   1:01 PM             11 Hello.txt
-a----        9/17/2017   1:06 PM            585 Hello.txt.encrypted
-a----        9/17/2017   1:08 PM             11 Hello.txt.encrypted.decrypted


PS C:\> Get-Content Hello.txt.encrypted.decrypted
Hello World
```

Mengenkripsi semua file dalam direktori

Contoh ini menggunakan CLI Enkripsi untuk mengenkripsi isi semua file dalam direktori. AWS

Ketika sebuah perintah mempengaruhi beberapa file, CLI AWS Enkripsi memproses setiap file satu per satu. Ini mendapatkan isi file, mendapatkan kunci data unik untuk file dari kunci master, mengenkripsi konten file di bawah kunci data, dan menulis hasilnya ke file baru di direktori output. Akibatnya, Anda dapat mendekripsi file output secara independen.

Daftar `TestDir` direktori ini menunjukkan file plaintext yang ingin kita enkripsi.

Bash

```
$  ls testdir
cool-new-thing.py  hello.txt  employees.csv
```

PowerShell

```
PS C:\> dir C:\TestDir

    Directory: C:\TestDir

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/12/2017   3:11 PM           2139 cool-new-thing.py
```

```
-a----        9/15/2017   5:57 PM             11 Hello.txt
-a----        9/17/2017   1:44 PM             46 Employees.csv
```

Perintah pertama menyimpan Amazon Resource Name (ARN) dari AWS KMS key variabel. `$keyArn`

Perintah kedua mengenkripsi konten file dalam `TestDir` direktori dan menulis file konten terenkripsi ke direktori. `TestEnc` Jika `TestEnc` direktori tidak ada, perintah gagal. Karena lokasi input adalah direktori, `--recursive` parameter diperlukan.

`--wrapping-keys`Parameter, dan atribut kunci yang diperlukan, tentukan kunci pembungkus yang akan digunakan. Perintah enkripsi mencakup konteks enkripsi,`dept=IT`. Saat Anda menentukan konteks enkripsi dalam perintah yang mengenkripsi beberapa file, konteks enkripsi yang sama digunakan untuk semua file.

Perintah ini juga memiliki `--metadata-output` parameter untuk memberi tahu CLI AWS Enkripsi tempat menulis metadata tentang operasi enkripsi. CLI AWS Enkripsi menulis satu catatan metadata untuk setiap file yang dienkripsi.

`--commitment-policy parameter`Ini opsional dimulai pada versi 2.1. x, tetapi disarankan. Jika perintah atau skrip gagal karena tidak dapat mendekripsi ciphertext, pengaturan kebijakan komitmen eksplisit dapat membantu Anda mendeteksi masalah dengan cepat.

Ketika perintah selesai, CLI AWS Enkripsi menulis file terenkripsi ke `TestEnc` direktori, tetapi tidak mengembalikan output apa pun.

Perintah terakhir mencantumkan file dalam `TestEnc` direktori. Ada satu file output dari konten terenkripsi untuk setiap file input konten plaintext. Karena perintah tidak menentukan akhiran alternatif, perintah enkripsi ditambahkan `.encrypted` ke masing-masing nama file input.

Bash

```
# To run this example, replace the fictitious key ARN with a valid master key
 identifier.
$  keyArn=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$ aws-encryption-cli --encrypt \
                     --input testdir --recursive\
                     --wrapping-keys key=$keyArn \
                     --encryption-context dept=IT \
```

```
                    --commitment-policy require-encrypt-require-decrypt \
                    --metadata-output ~/metadata \
                    --output testenc

$ ls testenc
cool-new-thing.py.encrypted  employees.csv.encrypted  hello.txt.encrypted
```

PowerShell

```
# To run this example, replace the fictitious key ARN with a valid master key
 identifier.
PS C:\> $keyArn = arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

PS C:\> aws-encryption-cli --encrypt `
                           --input .\TestDir --recursive `
                           --wrapping-keys key=$keyArn `
                           --encryption-context dept=IT `
                           --commitment-policy require-encrypt-require-decrypt `
                           --metadata-output .\Metadata\Metadata.txt `
                           --output .\TestEnc

PS C:\> dir .\TestEnc

    Directory: C:\TestEnc

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/17/2017   2:32 PM           2713 cool-new-thing.py.encrypted
-a----        9/17/2017   2:32 PM            620 Hello.txt.encrypted
-a----        9/17/2017   2:32 PM            585 Employees.csv.encrypted
```

Mendekripsi semua file dalam direktori

Contoh ini mendekripsi semua file dalam direktori. Dimulai dengan file di `TestEnc` direktori yang dienkripsi dalam contoh sebelumnya.

Bash

```
$  ls testenc
cool-new-thing.py.encrypted  hello.txt.encrypted  employees.csv.encrypted
```

PowerShell

```
PS C:\> dir C:\TestEnc

    Directory: C:\TestEnc

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/17/2017   2:32 PM           2713 cool-new-thing.py.encrypted
-a----        9/17/2017   2:32 PM            620 Hello.txt.encrypted
-a----        9/17/2017   2:32 PM            585 Employees.csv.encrypted
```

Perintah dekripsi ini mendekripsi semua file dalam TestEnc direktori dan menulis file plaintext ke direktori. TestDec `--wrapping-keys`Parameter dengan atribut kunci dan nilai ARN kunci memberi tahu AWS CLI Enkripsi yang akan digunakan AWS KMS keys untuk mendekripsi file. Perintah menggunakan `--interactive` parameter untuk memberi tahu CLI AWS Enkripsi untuk meminta Anda sebelum menimpa file dengan nama yang sama.

Perintah ini juga menggunakan konteks enkripsi yang disediakan saat file dienkripsi. Saat mendekripsi beberapa file, AWS CLI Enkripsi memeriksa konteks enkripsi setiap file. Jika pemeriksaan konteks enkripsi pada file apa pun gagal, CLI AWS Enkripsi menolak file, menulis peringatan, mencatat kegagalan dalam metadata, dan kemudian terus memeriksa file yang tersisa. Jika CLI AWS Enkripsi gagal mendekripsi file karena alasan lain, seluruh perintah dekripsi segera gagal.

Dalam contoh ini, pesan terenkripsi di semua file input berisi elemen konteks `dept=IT` enkripsi. Namun, jika Anda mendekripsi pesan dengan konteks enkripsi yang berbeda, Anda mungkin masih dapat memverifikasi bagian dari konteks enkripsi. Misalnya, jika beberapa pesan memiliki konteks enkripsi `dept=finance` dan yang lainnya memiliki`dept=IT`, Anda dapat memverifikasi bahwa konteks enkripsi selalu berisi `dept` nama tanpa menentukan nilainya. Jika Anda ingin lebih spesifik, Anda dapat mendekripsi file dalam perintah terpisah.

Perintah dekripsi tidak mengembalikan output apa pun, tetapi Anda dapat menggunakan perintah daftar direktori untuk melihat bahwa itu membuat file baru dengan akhiran. `.decrypted` Untuk melihat konten plaintext, gunakan perintah untuk mendapatkan konten file.

Bash

```
# To run this example, replace the fictitious key ARN with a valid master key
 identifier.
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$ aws-encryption-cli --decrypt \
                     --input testenc --recursive \
                     --wrapping-keys key=$keyArn \
                     --encryption-context dept=IT \
                     --commitment-policy require-encrypt-require-decrypt \
                     --metadata-output ~/metadata \
                     --max-encrypted-data-keys 1 \
                     --buffer \
                     --output testdec --interactive

$ ls testdec
cool-new-thing.py.encrypted.decrypted  hello.txt.encrypted.decrypted
 employees.csv.encrypted.decrypted
```

PowerShell

```
# To run this example, replace the fictitious key ARN with a valid master key
 identifier.
PS C:\> $keyArn = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

PS C:\> aws-encryption-cli --decrypt `
                           --input C:\TestEnc --recursive `
                           --wrapping-keys key=$keyArn `
                           --encryption-context dept=IT `
                           --commitment-policy require-encrypt-require-decrypt `
                           --metadata-output $home\Metadata.txt `
                           --max-encrypted-data-keys 1 `
                           --buffer `
                           --output C:\TestDec --interactive

PS C:\> dir .\TestDec


    Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
```

```
-a----        10/8/2017   4:57 PM           2139 cool-new-
thing.py.encrypted.decrypted
-a----        10/8/2017   4:57 PM             46 Employees.csv.encrypted.decrypted
-a----        10/8/2017   4:57 PM             11 Hello.txt.encrypted.decrypted
```

Mengenkripsi dan mendekripsi pada baris perintah

Contoh-contoh ini menunjukkan cara menyalurkan input ke perintah (stdin) dan menulis output ke baris perintah (stdout). Mereka menjelaskan cara merepresentasikan stdin dan stdout dalam sebuah perintah dan cara menggunakan alat pengkodean Base64 bawaan untuk mencegah shell salah menafsirkan karakter non-ASCII.

Contoh ini menyalurkan string teks biasa ke perintah enkripsi dan menyimpan pesan terenkripsi dalam variabel. Kemudian, ia menyalurkan pesan terenkripsi dalam variabel ke perintah dekripsi, yang menulis outputnya ke pipeline (stdout).

Contohnya terdiri dari tiga perintah:

- Perintah pertama menyimpan ARN kunci dari AWS KMS key variabel. `$keyArn`

  Bash

  ```
  $  keyArn=arn:aws:kms:us-
  west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
  ```

  PowerShell

  ```
  PS C:\> $keyArn = 'arn:aws:kms:us-
  west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
  ```

- Perintah kedua `Hello World` menyalurkan string ke perintah enkripsi dan menyimpan hasilnya dalam `$encrypted` variabel.

  `--output`Parameter `--input` dan diperlukan di semua perintah AWS Enkripsi CLI. Untuk menunjukkan bahwa input sedang disalurkan ke perintah (stdin), gunakan tanda hubung (`-`) untuk nilai parameter. `--input` Untuk mengirim output ke baris perintah (stdout), gunakan tanda hubung untuk nilai parameter. `--output`

`--encode`Parameter Base64-mengkodekan output sebelum mengembalikannya. Ini mencegah shell salah menafsirkan karakter non-ASCII dalam pesan terenkripsi.

Karena perintah ini hanyalah bukti konsep, kami menghilangkan konteks enkripsi dan menekan metadata (). `-S`

Bash

```
$ encrypted=$(echo 'Hello World' | aws-encryption-cli --encrypt -S \
                                                      --input - --output - --
encode \
                                                      --wrapping-keys key=
$keyArn )
```

PowerShell

```
PS C:\> $encrypted = 'Hello World' | aws-encryption-cli --encrypt -S `
                                                        --input - --output - --
encode `
                                                        --wrapping-keys key=
$keyArn
```

- Perintah ketiga menyalurkan pesan terenkripsi dalam `$encrypted` variabel ke perintah dekripsi.

  Perintah dekripsi ini digunakan `--input -` untuk menunjukkan bahwa input berasal dari pipeline (stdin) dan `--output -` untuk mengirim output ke pipeline (stdout). (Parameter input mengambil lokasi input, bukan byte input yang sebenarnya, sehingga Anda tidak dapat menggunakan `$encrypted` variabel sebagai nilai `--input` parameter.)

  Contoh ini menggunakan atribut penemuan `--wrapping-keys` parameter untuk memungkinkan CLI AWS Enkripsi menggunakan apapun AWS KMS key untuk mendekripsi data. Itu tidak menentukan kebijakan komitmen, sehingga menggunakan nilai default untuk versi 2.1. x dan kemudian, `require-encrypt-require-decrypt`

  Karena output dienkripsi dan kemudian dikodekan, perintah dekripsi menggunakan `--decode` parameter untuk memecahkan kode input yang dikodekan Base64 sebelum mendekripsi. Anda juga dapat menggunakan `--decode` parameter untuk memecahkan kode input yang dikodekan Base64 sebelum mengenkripsinya.

Sekali lagi, perintah menghilangkan konteks enkripsi dan menekan metadata (-). S

Bash

```
$  echo $encrypted | aws-encryption-cli --decrypt --wrapping-keys discovery=true
 --input - --output - --decode --buffer -S
Hello World
```

PowerShell

```
PS C:\> $encrypted | aws-encryption-cli --decrypt --wrapping-keys discovery=$true
 --input - --output - --decode --buffer -S
Hello World
```

Anda juga dapat melakukan operasi enkripsi dan dekripsi dalam satu perintah tanpa variabel intervensi.

Seperti pada contoh sebelumnya, `--output` parameter `--input` dan memiliki `-` nilai dan perintah menggunakan `--encode` parameter untuk menyandikan output dan `--decode` parameter untuk memecahkan kode input.

Bash

```
$  keyArn=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$  echo 'Hello World' |
          aws-encryption-cli --encrypt --wrapping-keys key=$keyArn --input - --
output - --encode -S |
          aws-encryption-cli --decrypt --wrapping-keys discovery=true --input - --
output - --decode -S
Hello World
```

PowerShell

```
PS C:\> $keyArn = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

PS C:\> 'Hello World' |
```

```
                aws-encryption-cli --encrypt --wrapping-keys key=$keyArn --input - --
output - --encode -S |
                aws-encryption-cli --decrypt --wrapping-keys discovery=$true --input
 - --output - --decode -S
Hello World
```

Menggunakan beberapa kunci master

Contoh ini menunjukkan cara menggunakan beberapa kunci master saat mengenkripsi dan mendekripsi data di CLI Enkripsi. AWS

Bila Anda menggunakan beberapa kunci master untuk mengenkripsi data, salah satu kunci master dapat digunakan untuk mendekripsi data. Strategi ini memastikan bahwa Anda dapat mendekripsi data bahkan jika salah satu kunci master tidak tersedia. Jika Anda menyimpan data terenkripsi dalam beberapa Wilayah AWS, strategi ini memungkinkan Anda menggunakan kunci master di Wilayah yang sama untuk mendekripsi data.

Saat Anda mengenkripsi dengan beberapa kunci master, kunci master pertama memainkan peran khusus. Ini menghasilkan kunci data yang digunakan untuk mengenkripsi data. Kunci master yang tersisa mengenkripsi kunci data teks biasa. Pesan terenkripsi yang dihasilkan mencakup data terenkripsi dan kumpulan kunci data terenkripsi, satu untuk setiap kunci master. Meskipun kunci master pertama menghasilkan kunci data, salah satu kunci master dapat mendekripsi salah satu kunci data, yang dapat digunakan untuk mendekripsi data.

Mengenkripsi dengan tiga kunci utama

Perintah contoh ini menggunakan tiga kunci pembungkus untuk mengenkripsi `Finance.log` file, satu di masing-masing tiga. Wilayah AWS

Ini menulis pesan terenkripsi ke direktori. `Archive` Perintah menggunakan `--suffix` parameter tanpa nilai untuk menekan akhiran, sehingga nama file input dan output akan sama.

Perintah menggunakan `--wrapping-keys` parameter dengan tiga atribut kunci. Anda juga dapat menggunakan beberapa `--wrapping-keys` parameter dalam perintah yang sama.

Untuk mengenkripsi file log, CLI AWS Enkripsi meminta kunci pembungkus pertama dalam daftar`$key1`,, untuk menghasilkan kunci data yang digunakannya untuk mengenkripsi data. Kemudian, ia menggunakan masing-masing kunci pembungkus lainnya untuk mengenkripsi salinan teks biasa dari kunci data yang sama. Pesan terenkripsi dalam file output mencakup ketiga kunci data terenkripsi.

Bash

```
$ key1=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
$ key2=arn:aws:kms:us-east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef
$ key3=arn:aws:kms:ap-
southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d

$ aws-encryption-cli --encrypt --input /logs/finance.log \
                               --output /archive --suffix \
                               --encryption-context class=log \
                               --metadata-output ~/metadata \
                               --wrapping-keys key=$key1 key=$key2 key=$key3
```

PowerShell

```
PS C:\> $key1 = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
PS C:\> $key2 = 'arn:aws:kms:us-
east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef'
PS C:\> $key3 = 'arn:aws:kms:ap-
southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d'

PS C:\> aws-encryption-cli --encrypt --input D:\Logs\Finance.log `
                           --output D:\Archive --suffix `
                           --encryption-context class=log `
                           --metadata-output $home\Metadata.txt `
                           --wrapping-keys key=$key1 key=$key2 key=$key3
```

Perintah ini mendekripsi salinan `Finance.log` file yang dienkripsi dan menulisnya ke `Finance.log.clear` file di direktori. `Finance` Untuk mendekripsi data yang dienkripsi di bawah tiga AWS KMS keys, Anda dapat menentukan tiga AWS KMS keys atau subset yang sama. Contoh ini hanya menentukan salah satu dari. AWS KMS keys

Untuk memberi tahu CLI AWS Enkripsi yang AWS KMS keys akan digunakan untuk mendekripsi data Anda, gunakan atribut kunci parameter. `--wrapping-keys` Saat mendekripsi dengan AWS KMS keys, nilai atribut kunci harus berupa ARN kunci.

Anda harus memiliki izin untuk memanggil Decrypt API pada yang AWS KMS keys Anda tentukan. Untuk informasi selengkapnya, lihat Otentikasi dan Kontrol Akses untuk AWS KMS.

Sebagai praktik terbaik, contoh ini menggunakan `--max-encrypted-data-keys` parameter untuk menghindari dekripsi pesan yang salah dengan jumlah kunci data terenkripsi yang berlebihan. Meskipun contoh ini hanya menggunakan satu kunci pembungkus untuk dekripsi, pesan terenkripsi memiliki tiga (3) kunci data terenkripsi; satu untuk masing-masing dari tiga kunci pembungkus yang digunakan saat mengenkripsi. Tentukan jumlah yang diharapkan dari kunci data terenkripsi atau nilai maksimum yang wajar, seperti 5. Jika Anda menentukan nilai maksimum kurang dari 3, perintah gagal. Lihat perinciannya di Membatasi kunci data terenkripsi.

Bash

```
$ aws-encryption-cli --decrypt --input /archive/finance.log \
                     --wrapping-keys key=$key1 \
                     --output /finance --suffix '.clear' \
                     --metadata-output ~/metadata \
                     --max-encrypted-data-keys 3 \
                     --buffer \
                     --encryption-context class=log
```

PowerShell

```
PS C:\> aws-encryption-cli --decrypt `
                           --input D:\Archive\Finance.log `
                           --wrapping-keys key=$key1 `
                           --output D:\Finance --suffix '.clear' `
                           --metadata-output .\Metadata\Metadata.txt `
                           --max-encrypted-data-keys 3 `
                           --buffer `
                           --encryption-context class=log
```

Mengenkripsi dan mendekripsi dalam skrip

Contoh ini menunjukkan cara menggunakan CLI AWS Enkripsi dalam skrip. Anda dapat menulis skrip yang hanya mengenkripsi dan mendekripsi data, atau skrip yang mengenkripsi atau mendekripsi sebagai bagian dari proses manajemen data.

Dalam contoh ini, skrip mendapatkan koleksi file log, mengompresnya, mengenkripsi mereka, dan kemudian menyalin file terenkripsi ke bucket Amazon S3. Skrip ini memproses setiap file secara terpisah, sehingga Anda dapat mendekripsi dan mengembangkannya secara independen.

Saat Anda mengompres dan mengenkripsi file, pastikan untuk mengompres sebelum Anda mengenkripsi. Data yang dienkripsi dengan benar tidak dapat dikompresi.

> **Warning**
>
> Hati-hati saat mengompresi data yang mencakup rahasia dan data yang mungkin dikendalikan oleh aktor jahat. Ukuran akhir dari data terkompresi mungkin secara tidak sengaja mengungkapkan informasi sensitif tentang isinya.

Bash

```
# Continue running even if an operation fails.
set +e

dir=$1
encryptionContext=$2
s3bucket=$3
s3folder=$4
masterKeyProvider="aws-kms"
metadataOutput="/tmp/metadata-$(date +%s)"

compress(){
    gzip -qf $1
}

encrypt(){
    # -e encrypt
    # -i input
    # -o output
    # --metadata-output unique file for metadata
    # -m masterKey read from environment variable
    # -c encryption context read from the second argument.
    # -v be verbose
    aws-encryption-cli -e -i ${1} -o $(dirname ${1}) --metadata-output
 ${metadataOutput} -m key="${masterKey}" provider="${masterKeyProvider}" -c
 "${encryptionContext}" -v
}


s3put (){
    # copy file argument 1 to s3 location passed into the script.
```

```
    aws s3 cp ${1} ${s3bucket}/${s3folder}
}

# Validate all required arguments are present.
if [ "${dir}" ] && [ "${encryptionContext}" ] && [ "${s3bucket}" ] &&
 [ "${s3folder}" ] && [ "${masterKey}" ]; then

# Is $dir a valid directory?
test -d "${dir}"
if [ $? -ne 0 ]; then
    echo "Input is not a directory; exiting"
    exit 1
fi

# Iterate over all the files in the directory, except *gz and *encrypted (in case of
 a re-run).
for f in $(find ${dir} -type f \( -name "*" ! -name \*.gz ! -name \*encrypted \) );
 do
    echo "Working on $f"
    compress ${f}
    encrypt ${f}.gz
    rm -f ${f}.gz
    s3put ${f}.gz.encrypted
done;
else
    echo "Arguments: <Directory> <encryption context> <s3://bucketname> <s3 folder>"
    echo " and ENV var \$masterKey must be set"
    exit 255
fi
```

PowerShell

```
#Requires -Modules AWSPowerShell, Microsoft.PowerShell.Archive
Param
(
    [Parameter(Mandatory)]
    [ValidateScript({Test-Path $_})]
    [String[]]
    $FilePath,

    [Parameter()]
    [Switch]
    $Recurse,
```

```
    [Parameter(Mandatory=$true)]
    [String]
    $wrappingKeyID,

    [Parameter()]
    [String]
    $masterKeyProvider = 'aws-kms',

    [Parameter(Mandatory)]
    [ValidateScript({Test-Path $_})]
    [String]
    $ZipDirectory,

    [Parameter(Mandatory)]
    [ValidateScript({Test-Path $_})]
    [String]
    $EncryptDirectory,

    [Parameter()]
    [String]
    $EncryptionContext,

    [Parameter(Mandatory)]
    [ValidateScript({Test-Path $_})]
    [String]
    $MetadataDirectory,

    [Parameter(Mandatory)]
    [ValidateScript({Test-S3Bucket -BucketName $_})]
    [String]
    $S3Bucket,

    [Parameter()]
    [String]
    $S3BucketFolder
)

BEGIN {}
PROCESS {
    if ($files = dir $FilePath -Recurse:$Recurse)
    {

        # Step 1: Compress
```

```
        foreach ($file in $files)
        {
            $fileName = $file.Name
            try
            {
                Microsoft.PowerShell.Archive\Compress-Archive -Path $file.FullName -
DestinationPath $ZipDirectory\$filename.zip
            }
            catch
            {
                Write-Error "Zip failed on $file.FullName"
            }

            # Step 2: Encrypt
            if (-not (Test-Path "$ZipDirectory\$filename.zip"))
            {
                Write-Error "Cannot find zipped file: $ZipDirectory\$filename.zip"
            }
            else
            {
                # 2>&1 captures command output
                $err = (aws-encryption-cli -e -i "$ZipDirectory\$filename.zip" `
                                           -o $EncryptDirectory `
                                           -m key=$wrappingKeyID provider=
$masterKeyProvider `
                                           -c $EncryptionContext `
                                           --metadata-output $MetadataDirectory `
                                           -v) 2>&1

                # Check error status
                if ($? -eq $false)
                {
                    # Write the error
                    $err
                }
                elseif (Test-Path "$EncryptDirectory\$fileName.zip.encrypted")
                {
                    # Step 3: Write to S3 bucket
                    if ($S3BucketFolder)
                    {
                        Write-S3Object -BucketName $S3Bucket -File
 "$EncryptDirectory\$fileName.zip.encrypted" -Key "$S3BucketFolder/
$fileName.zip.encrypted"
```

```
                    }
                    else
                    {
                        Write-S3Object -BucketName $S3Bucket -File
 "$EncryptDirectory\$fileName.zip.encrypted"
                    }
                }
            }
        }
    }
}
```

Menggunakan caching kunci data

Contoh ini menggunakan caching kunci data dalam perintah yang mengenkripsi sejumlah besar file.

Secara default, CLI AWS Enkripsi (dan versi lain dari AWS Encryption SDK) menghasilkan kunci data unik untuk setiap file yang dienkripsi. Meskipun menggunakan kunci data unik untuk setiap operasi adalah praktik terbaik kriptografi, penggunaan kembali kunci data yang terbatas dapat diterima untuk beberapa situasi. Jika Anda mempertimbangkan caching kunci data, konsultasikan dengan insinyur keamanan untuk memahami persyaratan keamanan aplikasi Anda dan tentukan ambang keamanan yang tepat untuk Anda.

Dalam contoh ini, caching kunci data mempercepat operasi enkripsi dengan mengurangi frekuensi permintaan ke penyedia kunci master.

Perintah dalam contoh ini mengenkripsi direktori besar dengan beberapa subdirektori yang berisi total sekitar 800 file log kecil. Perintah pertama menyimpan ARN dari AWS KMS key dalam variabel. `keyARN` Perintah kedua mengenkripsi semua file dalam direktori input (rekursif) dan menulisnya ke direktori arsip. Perintah menggunakan `--suffix` parameter untuk menentukan `.archive` sufiks.

`--caching`Parameter memungkinkan caching kunci data. Atribut kapasitas, yang membatasi jumlah kunci data dalam cache, diatur ke 1, karena pemrosesan file serial tidak pernah menggunakan lebih dari satu kunci data pada satu waktu. Atribut max_age, yang menentukan berapa lama kunci data cache dapat digunakan, diatur ke 10 detik.

Atribut max_messages_encrypted opsional disetel ke 10 pesan, sehingga satu kunci data tidak pernah digunakan untuk mengenkripsi lebih dari 10 file. Membatasi jumlah file yang dienkripsi oleh setiap kunci data mengurangi jumlah file yang akan terpengaruh jika kunci data dikompromikan.

Untuk menjalankan perintah ini pada file log yang dihasilkan sistem operasi Anda, Anda mungkin memerlukan izin administrator (sudodi Linux; Jalankan sebagai Administrator di Windows).

Bash

```
$  keyArn=arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

$  aws-encryption-cli --encrypt \
                      --input /var/log/httpd --recursive \
                      --output ~/archive --suffix .archive \
                      --wrapping-keys key=$keyArn \
                      --encryption-context class=log \
                      --suppress-metadata \
                      --caching capacity=1 max_age=10 max_messages_encrypted=10
```

PowerShell

```
PS C:\> $keyARN = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

PS C:\> aws-encryption-cli --encrypt `
                           --input C:\Windows\Logs --recursive `
                           --output $home\Archive --suffix '.archive' `
                           --wrapping-keys key=$keyARN `
                           --encryption-context class=log `
                           --suppress-metadata `
                           --caching capacity=1 max_age=10
 max_messages_encrypted=10
```

Untuk menguji efek caching kunci data, contoh ini menggunakan cmdlet Measure-Command in. PowerShell Ketika Anda menjalankan contoh ini tanpa caching kunci data, dibutuhkan sekitar 25 detik untuk menyelesaikannya. Proses ini menghasilkan kunci data baru untuk setiap file dalam direktori.

```
PS C:\> Measure-Command {aws-encryption-cli --encrypt `
                                            --input C:\Windows\Logs --recursive `
                                            --output $home\Archive  --suffix '.archive'
 `
                                            --wrapping-keys key=$keyARN `
                                            --encryption-context class=log `
                                            --suppress-metadata }
```

```
Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 25
Milliseconds      : 453
Ticks             : 254531202
TotalDays         : 0.000294596298611111
TotalHours        : 0.00707031116666667
TotalMinutes      : 0.42421867
TotalSeconds      : 25.4531202
TotalMilliseconds : 25453.1202
```

Caching kunci data membuat proses lebih cepat, bahkan ketika Anda membatasi setiap kunci data hingga maksimal 10 file. Perintah sekarang membutuhkan waktu kurang dari 12 detik untuk menyelesaikan dan mengurangi jumlah panggilan ke penyedia kunci master menjadi 1/10 dari nilai aslinya.

```
PS C:\> Measure-Command {aws-encryption-cli --encrypt `
                                            --input C:\Windows\Logs --recursive `
                                            --output $home\Archive  --suffix '.archive'
 `
                                            --wrapping-keys key=$keyARN `
                                            --encryption-context class=log `
                                            --suppress-metadata `
                                            --caching capacity=1 max_age=10
 max_messages_encrypted=10}


Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 11
Milliseconds      : 813
Ticks             : 118132640
TotalDays         : 0.000136727592592593
TotalHours        : 0.00328146222222222
TotalMinutes      : 0.196887733333333
TotalSeconds      : 11.813264
TotalMilliseconds : 11813.264
```

Jika Anda menghilangkan `max_messages_encrypted` batasan, semua file dienkripsi di bawah kunci data yang sama. Perubahan ini meningkatkan risiko menggunakan kembali kunci data tanpa membuat proses lebih cepat. Namun, ini mengurangi jumlah panggilan ke penyedia kunci master menjadi 1.

```
PS C:\> Measure-Command {aws-encryption-cli --encrypt `
                                            --input C:\Windows\Logs --recursive `
                                            --output $home\Archive  --suffix '.archive'
 `
                                            --wrapping-keys key=$keyARN `
                                            --encryption-context class=log `
                                            --suppress-metadata `
                                            --caching capacity=1 max_age=10}


Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 10
Milliseconds      : 252
Ticks             : 102523367
TotalDays         : 0.000118661304398148
TotalHours        : 0.00284787130555556
TotalMinutes      : 0.170872278333333
TotalSeconds      : 10.2523367
TotalMilliseconds : 10252.3367
```

AWS Encryption SDK Sintaks CLI dan referensi parameter

Topik ini menyediakan diagram sintaks dan deskripsi parameter singkat untuk membantu Anda menggunakan AWS Encryption SDK Command Line Interface (CLI). Untuk bantuan dengan kunci pembungkus dan parameter lainnya, lihatCara menggunakan CLI AWS Enkripsi. Sebagai contoh, lihat Contoh CLI AWS Enkripsi. Untuk dokumentasi selengkapnya, lihat Membaca Dokumen.

Topik

- AWS Sintaks CLI enkripsi
- AWS Parameter baris perintah CLI enkripsi
- Parameter lanjutan

AWS Sintaks CLI enkripsi

Diagram sintaks AWS Enkripsi CLI ini menunjukkan sintaks untuk setiap tugas yang Anda lakukan dengan CLI Enkripsi. AWS Mereka mewakili sintaks yang direkomendasikan dalam AWS Enkripsi CLI versi 2.1. x dan kemudian.

Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

> **Note**
>
> Kecuali dicatat dalam deskripsi parameter, setiap parameter atau atribut hanya dapat digunakan sekali dalam setiap perintah.
> Jika Anda menggunakan atribut yang parameter tidak mendukung, CLI AWS Enkripsi mengabaikan atribut yang tidak didukung tanpa peringatan atau kesalahan.

Mencari bantuan

Untuk mendapatkan sintaks AWS Enkripsi CLI lengkap dengan deskripsi parameter, gunakan atau. `--help` `-h`

```
aws-encryption-cli (--help | -h)
```

Dapatkan versinya

Untuk mendapatkan nomor versi instalasi CLI AWS Enkripsi Anda, gunakan. `--version` Pastikan untuk menyertakan versi saat Anda mengajukan pertanyaan, melaporkan masalah, atau berbagi tips tentang menggunakan CLI AWS Enkripsi.

```
aws-encryption-cli --version
```

Enkripsi data

Diagram sintaks berikut menunjukkan parameter yang digunakan encrypt perintah.

```
aws-encryption-cli --encrypt
                   --input <input> [--recursive] [--decode]
                   --output <output> [--interactive] [--no-overwrite] [--suffix
 [<suffix>]] [--encode]
```

```
                    --wrapping-keys  [--wrapping-keys] ...
                        key=<keyID> [key=<keyID>] ...
                        [provider=<provider-name>] [region=<aws-region>]
 [profile=<aws-profile>]
                    --metadata-output <location> [--overwrite-metadata] | --suppress-
metadata]
                    [--commitment-policy <commitment-policy>]
                    [--encryption-context <encryption_context> [<encryption_context>
 ...]]
                    [--max-encrypted-data-keys <integer>]
                    [--algorithm <algorithm_suite>]
                    [--caching <attributes>]
                    [--frame-length <length>]
                    [-v | -vv | -vvv | -vvvv]
                    [--quiet]
```

Dekripsi data

Diagram sintaks berikut menunjukkan parameter yang digunakan decrypt perintah.

Dalam versi 1.8. x, `--wrapping-keys` parameternya opsional saat mendekripsi, tetapi disarankan. Dimulai dari versi 2.1. x, `--wrapping-keys` parameter diperlukan saat mengenkripsi dan mendekripsi. Untuk AWS KMS keys, Anda dapat menggunakan atribut kunci untuk menentukan kunci pembungkus (praktik terbaik) atau menyetel atribut penemuan`true`, yang tidak membatasi kunci pembungkus yang dapat digunakan AWS CLI Enkripsi.

```
aws-encryption-cli --decrypt (or [--decrypt-unsigned])
                    --input <input> [--recursive] [--decode]
                    --output <output> [--interactive] [--no-overwrite]  [--suffix
 [<suffix>]] [--encode]
                    --wrapping-keys  [--wrapping-keys] ...
                        [key=<keyID>] [key=<keyID>] ...
                        [discovery={true|false}] [discovery-partition=<aws-partition-
name> discovery-account=<aws-account-ID> [discovery-account=<aws-account-ID>] ...]
                        [provider=<provider-name>] [region=<aws-region>]
 [profile=<aws-profile>]
                    --metadata-output <location> [--overwrite-metadata] | --suppress-
metadata]
                    [--commitment-policy <commitment-policy>]
                    [--encryption-context <encryption_context> [<encryption_context>
 ...]]
                    [--buffer]
                    [--max-encrypted-data-keys <integer>]
```

```
                    [--caching <attributes>]
                    [--max-length <length>]
                    [-v | -vv | -vvv | -vvvv]
                    [--quiet]
```

Gunakan file konfigurasi

Anda dapat merujuk ke file konfigurasi yang berisi parameter dan nilainya. Ini setara dengan mengetik parameter dan nilai dalam perintah. Sebagai contoh, lihat Cara menyimpan parameter dalam file konfigurasi.

```
aws-encryption-cli @<configuration_file>

# In a PowerShell console, use a backtick to escape the @.
aws-encryption-cli `@<configuration_file>
```

AWS Parameter baris perintah CLI enkripsi

Daftar ini memberikan deskripsi dasar parameter perintah AWS Enkripsi CLI. Untuk deskripsi lengkap, lihat aws-encryption-sdk-clidokumentasi.

--enkripsi (-e)

Mengenkripsi data input. Setiap perintah harus memiliki`--encrypt`, atau`--decrypt`, atau `--decrypt-unsigned` parameter.

--dekripsi (-d)

Mendekripsi data input. Setiap perintah harus memiliki`--encrypt`,`--decrypt`, atau `--decrypt-unsigned` parameter.

--decrypt-unsigned [Diperkenalkan dalam versi 1.9. x dan 2.2. x]

`--decrypt-unsigned`Parameter mendekripsi ciphertext dan memastikan bahwa pesan tidak ditandatangani sebelum dekripsi. Gunakan parameter ini jika Anda menggunakan `--algorithm` parameter dan memilih rangkaian algoritme tanpa penandatanganan digital untuk mengenkripsi data. Jika ciphertext ditandatangani, dekripsi gagal.

Anda dapat menggunakan `--decrypt` atau `--decrypt-unsigned` untuk dekripsi tetapi tidak keduanya.

--wrapping-keys (-w) [Diperkenalkan dalam versi 1.8. x]

Menentukan kunci pembungkus (atau kunci master) yang digunakan dalam operasi enkripsi dan dekripsi. Anda dapat menggunakan beberapa `--wrapping-keys` parameter di setiap perintah.

Dimulai dari versi 2.1. x, `--wrapping-keys` parameter diperlukan dalam perintah enkripsi dan dekripsi. Dalam versi 1.8. x, perintah enkripsi memerlukan salah satu `--wrapping-keys` atau `--master-keys` parameter. Dalam versi 1.8. x dekripsi perintah, `--wrapping-keys` parameter adalah opsional tetapi direkomendasikan.

Saat menggunakan penyedia kunci master kustom, perintah enkripsi dan dekripsi memerlukan atribut kunci dan penyedia. Saat menggunakan AWS KMS keys, perintah enkripsi memerlukan atribut kunci. Perintah dekripsi memerlukan atribut kunci atau atribut penemuan dengan nilai `true` (tetapi tidak keduanya). Menggunakan atribut kunci saat mendekripsi adalah praktik AWS Encryption SDK terbaik. Ini sangat penting jika Anda mendekripsi kumpulan pesan asing, seperti yang ada di bucket Amazon S3 atau antrian Amazon SQS.

Untuk contoh yang menunjukkan cara menggunakan kunci AWS KMS Multi-region sebagai kunci pembungkus, lihat. Menggunakan Multi-region AWS KMS keys

Atribut: Nilai `--wrapping-keys` parameter terdiri dari atribut berikut. Formatnya adalah `attribute_name=value`.

kunci

Mengidentifikasi kunci pembungkus yang digunakan dalam operasi. Formatnya adalah pasangan kunci = ID. Anda dapat menentukan beberapa atribut kunci di setiap nilai `--wrapping-keys` parameter.

- Enkripsi perintah: Semua perintah enkripsi memerlukan atribut kunci. Bila Anda menggunakan AWS KMS key dalam perintah enkripsi, nilai atribut kunci dapat berupa ID kunci, ARN kunci, nama alias, atau alias ARN. Untuk deskripsi pengidentifikasi AWS KMS kunci, lihat Pengidentifikasi kunci di Panduan Pengembang.AWS Key Management Service
- Dekripsi perintah: Saat mendekripsi dengan AWS KMS keys, `--wrapping-keys` parameter memerlukan atribut kunci dengan nilai ARN kunci atau atribut penemuan dengan nilai (tetapi tidak keduanya). `true` Menggunakan atribut kunci adalah praktik AWS Encryption SDK terbaik. Saat mendekripsi dengan penyedia kunci master kustom, atribut kunci diperlukan.

> **Note**
>
> Untuk menentukan kunci AWS KMS pembungkus dalam perintah dekripsi, nilai atribut kunci harus berupa ARN kunci. Jika Anda menggunakan ID kunci, nama alias, atau alias ARN, AWS CLI Enkripsi tidak mengenali kunci pembungkus.

Anda dapat menentukan beberapa atribut kunci di setiap nilai `--wrapping-keys` parameter. Namun, atribut penyedia, wilayah, dan profil apa pun dalam `--wrapping-keys` parameter berlaku untuk semua kunci pembungkus dalam nilai parameter tersebut. Untuk menentukan kunci pembungkus dengan nilai atribut yang berbeda, gunakan beberapa `--wrapping-keys` parameter dalam perintah.

penemuan

Memungkinkan CLI AWS Enkripsi menggunakan apapun AWS KMS key untuk mendekripsi pesan. Nilai penemuan bisa `true` atau`false`. Nilai default-nya adalah `false`. Atribut penemuan hanya valid dalam perintah dekripsi dan hanya jika penyedia kunci master berada. AWS KMS

Saat mendekripsi dengan AWS KMS keys, `--wrapping-keys` parameter memerlukan atribut kunci atau atribut penemuan dengan nilai `true` (tetapi tidak keduanya). Jika Anda menggunakan atribut kunci, Anda dapat menggunakan atribut penemuan dengan nilai `false` untuk secara eksplisit menolak penemuan.

- `False`(default) — Ketika atribut penemuan tidak ditentukan atau nilainya`false`, CLI AWS Enkripsi mendekripsi pesan hanya menggunakan yang AWS KMS keys ditentukan oleh atribut kunci parameter. `--wrapping-keys` Jika Anda tidak menentukan atribut kunci saat penemuan`false`, perintah dekripsi gagal. Nilai ini mendukung praktik terbaik CLI AWS Enkripsi.
- `True`— Ketika nilai atribut penemuan adalah`true`, CLI AWS Enkripsi mendapatkan metadata AWS KMS keys dari dalam pesan terenkripsi, dan menggunakannya untuk mendekripsi pesan. AWS KMS keys Atribut penemuan dengan nilai `true` berperilaku seperti versi CLI AWS Enkripsi sebelum versi 1.8. x yang tidak mengizinkan Anda menentukan kunci pembungkus saat mendekripsi. Namun, maksud Anda untuk menggunakan apapun AWS KMS key adalah eksplisit. Jika Anda menentukan atribut kunci saat penemuan`true`, perintah dekripsi gagal.

`true`Nilai tersebut dapat menyebabkan CLI AWS Enkripsi digunakan AWS KMS keys di berbagai Wilayah Akun AWS dan yang berbeda, atau mencoba menggunakan AWS KMS keys yang tidak diizinkan untuk digunakan oleh pengguna.

Saat penemuan dilakukan**`true`**, sebaiknya gunakan atribut partisi penemuan dan akun-penemuan untuk membatasi atribut yang AWS KMS keys digunakan pada atribut yang Anda tentukan. Akun AWS

penemuan-akun

Membatasi yang AWS KMS keys digunakan untuk mendekripsi ke yang ditentukan. Akun AWS Satu-satunya nilai yang valid untuk atribut ini adalah Akun AWS ID.

Atribut ini opsional dan hanya valid dalam perintah dekripsi dengan AWS KMS keys tempat atribut penemuan diatur `true` dan atribut partisi penemuan ditentukan.

Setiap atribut discovery-account hanya membutuhkan satu Akun AWS ID, tetapi Anda dapat menentukan beberapa atribut discovery-account dalam parameter yang sama. `--wrapping-keys` Semua akun yang ditentukan dalam `--wrapping-keys` parameter tertentu harus berada di AWS partisi yang ditentukan.

penemuan-partisi

Menentukan AWS partisi untuk account di atribut discovery-account. Nilainya harus berupa AWS partisi, seperti`aws`,`aws-cn`, atau`aws-gov-cloud`. Untuk selengkapnya, lihat Nama Sumber Daya Amazon di Referensi Umum AWS.

Atribut ini diperlukan saat Anda menggunakan atribut discovery-account. Anda hanya dapat menentukan satu atribut partisi penemuan di setiap parameter. `--wrapping keys` Untuk menentukan Akun AWS di beberapa partisi, gunakan `--wrapping-keys` parameter tambahan.

penyedia

Mengidentifikasi penyedia kunci utama. Formatnya adalah penyedia = pasangan ID. Nilai default, aws-kms, mewakili. AWS KMS Atribut ini diperlukan hanya jika penyedia kunci master tidak AWS KMS.

region

Mengidentifikasi Wilayah AWS dari sebuah AWS KMS key. Atribut ini hanya berlaku untuk AWS KMS keys. Ini hanya digunakan ketika pengidentifikasi kunci tidak menentukan Wilayah;

jika tidak, itu diabaikan. Ketika digunakan, itu mengganti Wilayah default di profil bernama AWS CLI.

profile

Mengidentifikasi profil AWS CLI bernama. Atribut ini hanya berlaku untuk AWS KMS keys. Wilayah di profil hanya digunakan ketika pengidentifikasi kunci tidak menentukan Wilayah dan tidak ada atribut wilayah dalam perintah.

--masukan (-i)

Menentukan lokasi data untuk mengenkripsi atau mendekripsi. Parameter ini diperlukan. Nilai dapat berupa jalur ke file atau direktori, atau pola nama file. Jika Anda menyalurkan input ke perintah (stdin), gunakan. `-`

Jika input tidak ada, perintah selesai dengan sukses tanpa kesalahan atau peringatan.

--rekursif (-r, -R)

Melakukan operasi pada file di direktori input dan subdirektorinya. Parameter ini diperlukan ketika nilai `--input` adalah direktori.

--decode

Mendekode masukan yang dikodekan Base64.

Jika Anda mendekripsi pesan yang dienkripsi dan kemudian dikodekan, Anda harus memecahkan kode pesan sebelum mendekripsi. Parameter ini melakukan itu untuk Anda.

Misalnya, jika Anda menggunakan `--encode` parameter dalam perintah enkripsi, gunakan `--decode` parameter dalam perintah dekripsi yang sesuai. Anda juga dapat menggunakan parameter ini untuk memecahkan kode input yang dikodekan Base64 sebelum Anda mengenkripsinya.

--keluaran (-o)

Menentukan tujuan untuk output. Parameter ini diperlukan. Nilai dapat berupa nama file, direktori yang ada, atau`-`, yang menulis output ke baris perintah (stdout).

Jika direktori output yang ditentukan tidak ada, perintah gagal. Jika input berisi subdirektori, AWS CLI Enkripsi mereproduksi subdirektori di bawah direktori output yang Anda tentukan.

Secara default, CLI AWS Enkripsi menimpa file dengan nama yang sama. Untuk mengubah perilaku itu, gunakan `--no-overwrite` parameter `--interactive` atau. Untuk menekan peringatan penimpaan, gunakan parameter. `--quiet`

> **Note**
>
> Jika perintah yang akan menimpa file output gagal, file output dihapus.

--interaktif

Meminta sebelum menimpa file.

--tidak menimpa

Tidak menimpa file. Sebaliknya, jika file output ada, CLI AWS Enkripsi melewatkan input yang sesuai.

--akhiran

Menentukan akhiran nama file kustom untuk file yang dibuat AWS CLI Enkripsi. Untuk menunjukkan tidak ada akhiran, gunakan parameter tanpa nilai (`--suffix`).

Secara default, ketika `--output` parameter tidak menentukan nama file, nama file output memiliki nama yang sama dengan nama file input ditambah akhiran. Sufiks untuk perintah enkripsi adalah. `.encrypted` Sufiks untuk perintah dekripsi adalah. `.decrypted`

--enkode

Menerapkan pengkodean Base64 (biner ke teks) ke output. Pengkodean mencegah program host shell salah menafsirkan karakter non-ASCII dalam teks keluaran.

Gunakan parameter ini saat menulis output terenkripsi ke stdout (`--output -`), terutama di PowerShell konsol, bahkan saat Anda menyalurkan output ke perintah lain atau menyimpannya dalam variabel.

--metadata-keluaran

Menentukan lokasi untuk metadata tentang operasi kriptografi. Masukkan jalur dan nama file. Jika direktori tidak ada, perintah gagal. Untuk menulis metadata ke baris perintah (stdout), gunakan. `-`

Anda tidak dapat menulis perintah output (`--output`) dan metadata output (`--metadata-output`) ke stdout dalam perintah yang sama. Juga, ketika nilai `--input` atau `--output` adalah direktori (tanpa nama file), Anda tidak dapat menulis keluaran metadata ke direktori yang sama atau ke subdirektori mana pun dari direktori itu.

Jika Anda menentukan file yang ada, secara default, CLI AWS Enkripsi menambahkan catatan metadata baru ke konten apa pun dalam file. Fitur ini memungkinkan Anda membuat satu file

yang berisi metadata untuk semua operasi kriptografi Anda. Untuk menimpa konten dalam file yang ada, gunakan `--overwrite-metadata` parameter.

CLI AWS Enkripsi mengembalikan catatan metadata berformat JSON untuk setiap operasi enkripsi atau dekripsi yang dilakukan perintah. Setiap catatan metadata mencakup jalur lengkap ke file input dan output, konteks enkripsi, rangkaian algoritme, dan informasi berharga lainnya yang dapat Anda gunakan untuk meninjau operasi dan memverifikasi bahwa itu memenuhi standar keamanan Anda.

--timpa metadata

Menimpa konten dalam file keluaran metadata. Secara default, `--metadata-output` parameter menambahkan metadata ke konten yang ada dalam file.

--menekan-metadata (-S)

Menekan metadata tentang operasi enkripsi atau dekripsi.

--komitmen-kebijakan

Menentukan kebijakan komitmen untuk mengenkripsi dan mendekripsi perintah. Kebijakan komitmen menentukan apakah pesan Anda dienkripsi dan didekripsi dengan fitur keamanan komitmen utama.

`--commitment-policy`Parameter diperkenalkan dalam versi 1.8. x. Ini berlaku dalam perintah enkripsi dan dekripsi.

Dalam versi 1.8. x, CLI AWS Enkripsi menggunakan kebijakan `forbid-encrypt-allow-decrypt` komitmen untuk semua operasi enkripsi dan dekripsi. Bila Anda menggunakan `--wrapping-keys` parameter dalam perintah enkripsi atau dekripsi, `--commitment-policy` parameter dengan `forbid-encrypt-allow-decrypt` nilai diperlukan. Jika Anda tidak menggunakan `--wrapping-keys` parameter, `--commitment-policy` parameter tidak valid. Menetapkan kebijakan komitmen secara eksplisit mencegah kebijakan komitmen Anda berubah secara otomatis menjadi `require-encrypt-require-decrypt` saat Anda meningkatkan ke versi 2.1. x

Dimulai pada versi 2.1. x, semua nilai kebijakan komitmen didukung. `--commitment-policy`Parameternya opsional dan nilai defaultnya adalah`require-encrypt-require-decrypt`.

Parameter ini memiliki nilai-nilai berikut:

- `forbid-encrypt-allow-decrypt`— Tidak dapat mengenkripsi dengan komitmen utama. Ini dapat mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen utama.

  Dalam versi 1.8. x, ini adalah satu-satunya nilai yang valid. CLI AWS Enkripsi menggunakan kebijakan `forbid-encrypt-allow-decrypt` komitmen untuk semua operasi enkripsi dan dekripsi.
- `require-encrypt-allow-decrypt`— Enkripsi hanya dengan komitmen utama. Mendekripsi dengan dan tanpa komitmen utama. Nilai ini diperkenalkan dalam versi 2.1. x.
- `require-encrypt-require-decrypt`(default) — Mengenkripsi dan mendekripsi hanya dengan komitmen utama. Nilai ini diperkenalkan dalam versi 2.1. x. Ini adalah nilai default dalam versi 2.1. x dan kemudian. Dengan nilai ini, CLI AWS Enkripsi tidak akan mendekripsi ciphertext apa pun yang dienkripsi dengan versi sebelumnya. AWS Encryption SDK

Untuk informasi terperinci tentang menetapkan kebijakan komitmen Anda, lihatMigrasi Anda AWS Encryption SDK.

--enkripsi-konteks (-c)

Menentukan konteks enkripsi untuk operasi. Parameter ini tidak diperlukan, tetapi disarankan.

- Dalam sebuah `--encrypt` perintah, masukkan satu atau lebih `name=value` pasangan. Gunakan spasi untuk memisahkan pasangan.
- Dalam sebuah `--decrypt` perintah, masukkan `name=value` pasangan, `name` elemen tanpa nilai, atau keduanya.

Jika `name` atau `value` dalam `name=value` pasangan menyertakan spasi atau karakter khusus, lampirkan seluruh pasangan dalam tanda kutip. Misalnya, `--encryption-context "department=software development"`.

--buffer (-b) [Diperkenalkan dalam versi 1.9. x dan 2.2. x]

Mengembalikan plaintext hanya setelah semua input diproses, termasuk memverifikasi tanda tangan digital jika ada.

-- max-encrypted-data-keys [Diperkenalkan dalam versi 1.9. x dan 2.2. x]

Menentukan jumlah maksimum kunci data terenkripsi dalam pesan terenkripsi. Parameter ini bersifat opsional.

Nilai yang valid adalah 1 - 65.535. Jika Anda menghilangkan parameter ini, CLI AWS Enkripsi tidak memberlakukan maksimum apa pun. Pesan terenkripsi dapat menampung hingga 65.535 (2^16 - 1) kunci data terenkripsi.

Anda dapat menggunakan parameter ini dalam perintah enkripsi untuk mencegah pesan yang salah. Anda dapat menggunakannya dalam perintah dekripsi untuk mendeteksi pesan berbahaya dan menghindari mendekripsi pesan dengan banyak kunci data terenkripsi yang tidak dapat Anda dekripsi. Untuk detail dan contoh, lihat Membatasi kunci data terenkripsi.

--bantuan (-h)

Mencetak penggunaan dan sintaks pada baris perintah.

--versi

Mendapat versi CLI AWS Enkripsi.

-v | -vv | -vvv | -vvv

Menampilkan informasi verbose, peringatan, dan pesan debugging. Detail dalam output meningkat dengan jumlah `v` s dalam parameter. Setelan (`-vvvv`) yang paling rinci mengembalikan data tingkat debugging dari AWS CLI Enkripsi dan semua komponen yang digunakannya.

--tenang (-q)

Menekan pesan peringatan, seperti pesan yang muncul saat Anda menimpa file keluaran.

--master-keys (-m) [Usang]

> **Note**
>
> Parameter --master-keys tidak digunakan lagi di 1.8. x dan dihapus dalam versi 2.1. x. Sebagai gantinya, gunakan parameter --wrapping-keys.

Menentukan kunci master yang digunakan dalam operasi enkripsi dan dekripsi. Anda dapat menggunakan beberapa parameter kunci master di setiap perintah.

`--master-keys`Parameter diperlukan dalam perintah enkripsi. Ini diperlukan dalam perintah dekripsi hanya ketika Anda menggunakan penyedia kunci master kustom (non-#-AWS KMS).

Atribut: Nilai `--master-keys` parameter terdiri dari atribut berikut. Formatnya adalah `attribute_name=value`.

kunci

Mengidentifikasi kunci pembungkus yang digunakan dalam operasi. Formatnya adalah pasangan kunci = ID. Atribut kunci diperlukan di semua perintah enkripsi.

Bila Anda menggunakan AWS KMS key dalam perintah enkripsi, nilai atribut kunci dapat berupa ID kunci, ARN kunci, nama alias, atau alias ARN. Untuk detail tentang pengidentifikasi AWS KMS kunci, lihat Pengidentifikasi kunci di Panduan AWS Key Management Service Pengembang.

Atribut kunci diperlukan dalam perintah dekripsi ketika penyedia kunci master tidak. AWS KMS Atribut kunci tidak diizinkan dalam perintah yang mendekripsi data yang dienkripsi di bawah file. AWS KMS key

Anda dapat menentukan beberapa atribut kunci di setiap nilai `--master-keys` parameter. Namun, atribut penyedia, wilayah, dan profil apa pun berlaku untuk semua kunci master dalam nilai parameter. Untuk menentukan kunci master dengan nilai atribut yang berbeda, gunakan beberapa `--master-keys` parameter dalam perintah.

penyedia

Mengidentifikasi penyedia kunci utama. Formatnya adalah penyedia = pasangan ID. Nilai default, aws-kms, mewakili. AWS KMS Atribut ini diperlukan hanya jika penyedia kunci master tidak AWS KMS.

region

Mengidentifikasi Wilayah AWS dari sebuah AWS KMS key. Atribut ini hanya berlaku untuk AWS KMS keys. Ini hanya digunakan ketika pengidentifikasi kunci tidak menentukan Wilayah; jika tidak, itu diabaikan. Ketika digunakan, itu mengganti Wilayah default di profil bernama AWS CLI.

profile

Mengidentifikasi profil AWS CLI bernama. Atribut ini hanya berlaku untuk AWS KMS keys. Wilayah di profil hanya digunakan ketika pengidentifikasi kunci tidak menentukan Wilayah dan tidak ada atribut wilayah dalam perintah.

Parameter lanjutan

--algoritma

Menentukan suite algoritma alternatif. Parameter ini opsional dan hanya valid dalam perintah enkripsi.

Jika Anda menghilangkan parameter ini, CLI AWS Enkripsi menggunakan salah satu rangkaian algoritme default untuk yang diperkenalkan AWS Encryption SDK di versi 1.8. x. Kedua algoritma

default menggunakan AES-GCM dengan HKDF, tanda tangan ECDSA, dan kunci enkripsi 256-bit. Seseorang menggunakan komitmen utama; yang satu tidak. Pilihan rangkaian algoritma default ditentukan oleh kebijakan komitmen untuk perintah.

Suite algoritma default direkomendasikan untuk sebagian besar operasi enkripsi. Untuk daftar nilai yang valid, lihat nilai untuk `algorithm` parameter di Baca Dokumen.

--bingkai-panjang

Menciptakan output dengan panjang bingkai yang ditentukan. Parameter ini opsional dan hanya valid dalam perintah enkripsi.

Masukkan nilai dalam byte. Nilai yang valid adalah 0 dan 1 - 2^31 - 1. Nilai 0 menunjukkan data yang tidak dibingkai. Defaultnya adalah 4096 (byte).

> **Note**
>
> Bila memungkinkan, gunakan data berbingkai. AWS Encryption SDK Mendukung data nonframed hanya untuk penggunaan lama. Beberapa implementasi bahasa masih AWS Encryption SDK dapat menghasilkan ciphertext nonframed. Semua implementasi bahasa yang didukung dapat mendekripsi ciphertext berbingkai dan nonframed.

--max-panjang

Menunjukkan ukuran bingkai maksimum (atau panjang konten maksimum untuk pesan yang tidak dibingkai) dalam byte untuk dibaca dari pesan terenkripsi. Parameter ini opsional dan hanya valid dalam perintah dekripsi. Ini dirancang untuk melindungi Anda dari mendekripsi ciphertext berbahaya yang sangat besar.

Masukkan nilai dalam byte. Jika Anda menghilangkan parameter ini, AWS Encryption SDK tidak membatasi ukuran bingkai saat mendekripsi.

--caching

Mengaktifkan fitur caching kunci data, yang menggunakan kembali kunci data, alih-alih menghasilkan kunci data baru untuk setiap file input. Parameter ini mendukung skenario lanjutan. Pastikan untuk membaca dokumentasi Data Key Caching sebelum menggunakan fitur ini.

`--caching`Parameter memiliki atribut berikut.

kapasitas (diperlukan)

Menentukan jumlah maksimum entri dalam cache.

Nilai minimum adalah 1. Tidak ada nilai maksimum.

max_age (wajib)

Tentukan berapa lama entri cache digunakan, dalam hitungan detik, dimulai saat ditambahkan ke cache.

Masukkan nilai yang lebih besar dari 0. Tidak ada nilai maksimum.

max_messages_encrypted (opsional)

Menentukan jumlah maksimum pesan yang dapat dienkripsi oleh entri cache.

Nilai yang valid adalah 1 - 2 ^ 32. Nilai default adalah 2 ^ 32 (pesan).

max_bytes_encrypted (opsional)

Menentukan jumlah maksimum byte yang dapat dienkripsi oleh entri yang di-cache.

Nilai yang valid adalah 0 dan 1 - 2^63 - 1. Nilai default adalah 2 ^ 63 - 1 (pesan). Nilai 0 memungkinkan Anda menggunakan caching kunci data hanya ketika Anda mengenkripsi string pesan kosong.

Versi CLI AWS Enkripsi

Kami menyarankan Anda menggunakan CLI AWS Enkripsi versi terbaru.

> **Note**
>
> Versi CLI AWS Enkripsi lebih awal dari 4.0.0 sedang dalam fase. end-of-support
> Anda dapat memperbarui dengan aman dari versi 2.1. x dan yang lebih baru ke versi terbaru CLI AWS Enkripsi tanpa perubahan kode atau data apa pun. Namun, fitur keamanan baru diperkenalkan di versi 2.1. x tidak kompatibel ke belakang. Untuk memperbarui dari versi 1.7. x atau sebelumnya, Anda harus terlebih dahulu memperbarui ke yang terbaru 1. x versi CLI AWS Enkripsi. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.
> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x

menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Untuk informasi tentang versi signifikan dari AWS Encryption SDK, lihatVersi dari AWS Encryption SDK.

Versi mana yang saya gunakan?

Jika Anda baru mengenal CLI AWS Enkripsi, gunakan versi terbaru.

Untuk mendekripsi data yang dienkripsi oleh versi AWS Encryption SDK sebelumnya dari versi 1.7. x, migrasi terlebih dahulu ke versi terbaru dari CLI AWS Enkripsi. Buat semua perubahan yang disarankan sebelum memperbarui ke versi 2.1. x atau yang lebih baru. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

Pelajari selengkapnya

- Untuk informasi terperinci tentang perubahan dan panduan untuk bermigrasi ke versi baru ini, lihatMigrasi Anda AWS Encryption SDK.
- Untuk deskripsi parameter dan atribut CLI AWS Enkripsi baru, lihat. AWS Encryption SDK Sintaks CLI dan referensi parameter

Daftar berikut menjelaskan perubahan CLI AWS Enkripsi di versi 1.8. x dan 2.1. x.

Versi 1.8. x perubahan pada CLI AWS Enkripsi

- Menghentikan parameter. `--master-keys` Sebagai gantinya, gunakan `--wrapping-keys` parameternya.
- Menambahkan parameter `--wrapping-keys` (`-w`). Ini mendukung semua atribut `--master-keys` parameter. Ini juga menambahkan atribut opsional berikut, yang hanya valid saat mendekripsi dengan. AWS KMS keys
  - penemuan
  - penemuan-partisi
  - penemuan-akun

  Untuk penyedia kunci master kustom, `--encrypt` dan - `-decrypt` perintah memerlukan `--wrapping-keys` parameter atau `--master-keys` parameter (tetapi tidak keduanya). Juga, `--`

`encrypt` perintah dengan AWS KMS keys membutuhkan `--wrapping-keys` parameter atau `--master-keys` parameter (tetapi tidak keduanya).

Dalam `--decrypt` perintah dengan AWS KMS keys, `--wrapping-keys` parameternya opsional, tetapi disarankan, karena diperlukan dalam versi 2.1. x. Jika Anda menggunakannya, Anda harus menentukan atribut kunci atau atribut penemuan dengan nilai `true` (tetapi tidak keduanya).

- Menambahkan `--commitment-policy` parameter. Satu-satunya nilai yang valid adalah `forbid-encrypt-allow-decrypt`. Kebijakan `forbid-encrypt-allow-decrypt` komitmen digunakan dalam semua perintah enkripsi dan dekripsi.

  Dalam versi 1.8. x, ketika Anda menggunakan `--wrapping-keys` parameter, `--commitment-policy` parameter dengan `forbid-encrypt-allow-decrypt` nilai diperlukan. Menyetel nilai secara eksplisit mencegah kebijakan komitmen Anda berubah secara otomatis menjadi `require-encrypt-require-decrypt` saat Anda meningkatkan ke versi 2.1. x.

Versi 2.1. x perubahan pada CLI AWS Enkripsi

- Menghapus `--master-keys` parameter. Sebagai gantinya, gunakan `--wrapping-keys` parameternya.
- `--wrapping-keys`Parameter diperlukan di semua perintah enkripsi dan dekripsi. Anda harus menentukan atribut kunci atau atribut penemuan dengan nilai `true` (tetapi tidak keduanya).
- `--commitment-policy`Parameter mendukung nilai-nilai berikut. Lihat perinciannya di Menetapkan kebijakan komitmen Anda.
  - `forbid-encrypt-allow-decrypt`
  - `require-encrypt-allow-decrypt`
  - `require-encrypt-require decrypt`(Default)
- `--commitment-policy`Parameternya opsional di versi 2.1. x. Nilai default-nya adalah `require-encrypt-require-decrypt`.

Versi 1.9. x dan 2.2. x perubahan pada CLI AWS Enkripsi

- Menambahkan `--decrypt-unsigned` parameter. Lihat perinciannya di Versi 2.2. x.
- Menambahkan `--buffer` parameter. Lihat perinciannya di Versi 2.2. x.
- Menambahkan `--max-encrypted-data-keys` parameter. Lihat perinciannya di Membatasi kunci data terenkripsi.

Versi 3.0. x perubahan pada CLI AWS Enkripsi

- Menambahkan dukungan untuk kunci AWS KMS Multi-wilayah. Lihat perinciannya di Menggunakan Multi-region AWS KMS keys.

Caching kunci data

Caching kunci data menyimpan kunci data dan materi kriptografi terkait dalam cache. Ketika Anda mengenkripsi atau mendekripsi data, AWS Encryption SDK mencari kunci data yang cocok dalam cache. Jika menemukan kecocokan, ia menggunakan kunci data yang di-cache daripada menghasilkan yang baru. Caching kunci data dapat meningkatkan kinerja, mengurangi biaya, dan membantu Anda tetap dalam batas layanan saat aplikasi Anda meningkat.

Aplikasi Anda dapat memperoleh manfaat dari caching kunci data jika:

- Itu dapat menggunakan kembali kunci data.
- Ini menghasilkan banyak kunci data.
- Operasi kriptografi Anda sangat lambat, mahal, terbatas, atau intensif sumber daya.

Caching dapat mengurangi penggunaan layanan kriptografi Anda, seperti AWS Key Management Service ()AWS KMS. Jika Anda mencapai AWS KMS requests-per-secondbatas Anda, caching dapat membantu. Aplikasi Anda dapat menggunakan kunci cache untuk melayani beberapa permintaan kunci data Anda alih-alih menelepon AWS KMS. (Anda juga dapat membuat kasus di AWS Support Center untuk menaikkan batas akun Anda.)

AWS Encryption SDK Ini membantu Anda membuat dan mengelola cache kunci data Anda. Ini menyediakan cache lokal dan manajer bahan kriptografi caching (caching CMM) yang berinteraksi dengan cache dan memberlakukan ambang keamanan yang Anda tetapkan. Bekerja sama, komponen-komponen ini membantu Anda mendapatkan keuntungan dari efisiensi penggunaan kembali kunci data sambil menjaga keamanan sistem Anda.

Caching kunci data adalah fitur opsional AWS Encryption SDK yang harus Anda gunakan dengan hati-hati. Secara default, AWS Encryption SDK menghasilkan kunci data baru untuk setiap operasi enkripsi. Teknik ini mendukung praktik terbaik kriptografi, yang mencegah penggunaan kembali kunci data yang berlebihan. Secara umum, gunakan caching kunci data hanya jika diperlukan untuk memenuhi tujuan kinerja Anda. Kemudian, gunakan ambang keamanan caching kunci data untuk memastikan bahwa Anda menggunakan jumlah minimum caching yang diperlukan untuk memenuhi tujuan biaya dan kinerja Anda.

Versi 3. x dari AWS Encryption SDK for Java satu-satunya mendukung CMM caching dengan antarmuka penyedia kunci master lama, bukan antarmuka keyring. Namun, versi 4. x dari AWS Encryption SDK untuk .NET, versi 3. x dari AWS Encryption SDK for Java, versi 4. x dari AWS

Encryption SDK for Python, versi 1. x dari AWS Encryption SDK untuk Rust dan versi 0.1. x atau yang lebih baru dari AWS Encryption SDK for Go mendukung keyring AWS KMS Hierarchical, solusi caching bahan kriptografi alternatif. Konten yang dienkripsi dengan keyring AWS KMS Hierarkis hanya dapat didekripsi dengan keyring Hierarkis. AWS KMS

Untuk diskusi rinci tentang pengorbanan keamanan ini, lihat AWS Encryption SDK: Cara Memutuskan apakah Caching Kunci Data Tepat untuk Aplikasi Anda di Blog Keamanan. AWS

Topik

- Cara menggunakan caching kunci data
- Mengatur ambang keamanan cache
- Detail caching kunci data
- Contoh caching kunci data

Cara menggunakan caching kunci data

Topik ini menunjukkan cara menggunakan caching kunci data dalam aplikasi Anda. Ini membawa Anda melalui proses langkah demi langkah. Kemudian, ia menggabungkan langkah-langkah dalam contoh sederhana yang menggunakan caching kunci data dalam operasi untuk mengenkripsi string.

Contoh di bagian ini menunjukkan cara menggunakan versi 2.0. x dan yang lebih baru AWS Encryption SDK. Untuk contoh yang menggunakan versi sebelumnya, temukan rilis Anda di daftar Rilis GitHub repositori untuk bahasa pemrograman Anda.

Untuk contoh lengkap dan teruji menggunakan caching kunci data di AWS Encryption SDK, lihat:

- C/C++: caching_cmm.cpp
- Jawa: SimpleDataKeyCachingExample.java
- JavaScript Peramban: caching_cmm.ts
- JavaScript Node.js: caching_cmm.ts
- Python: data_key_caching_basic.py

AWS Encryption SDK Untuk .NET tidak mendukung caching kunci data.

Topik

- Menggunakan caching kunci data: Step-by-step

- Contoh caching kunci data: Enkripsi string

Menggunakan caching kunci data: Step-by-step

step-by-stepPetunjuk ini menunjukkan cara membuat komponen yang Anda butuhkan untuk mengimplementasikan caching kunci data.

- Buat cache kunci data. Dalam contoh ini, kami menggunakan cache lokal yang AWS Encryption SDK disediakan. Kami membatasi cache hingga 10 kunci data.

C

```
// Cache capacity (maximum number of entries) is required
size_t cache_capacity = 10;
struct aws_allocator *allocator = aws_default_allocator();

struct aws_cryptosdk_materials_cache *cache =
 aws_cryptosdk_materials_cache_local_new(allocator, cache_capacity);
```

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x dari CMM AWS Encryption SDK for Java caching kunci data tidak digunakan lagi. Dengan versi 3. x, Anda juga dapat menggunakan keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

```
// Cache capacity (maximum number of entries) is required
int MAX_CACHE_SIZE = 10;

CryptoMaterialsCache cache = new LocalCryptoMaterialsCache(MAX_CACHE_SIZE);
```

JavaScript Browser

```
const capacity = 10

const cache = getLocalCryptographicMaterialsCache(capacity)
```

JavaScript Node.js

```
const capacity = 10

const cache = getLocalCryptographicMaterialsCache(capacity)
```

Python

```
# Cache capacity (maximum number of entries) is required
MAX_CACHE_SIZE = 10

cache = aws_encryption_sdk.LocalCryptoMaterialsCache(MAX_CACHE_SIZE)
```

- Buat penyedia kunci master (Java dan Python) atau keyring (C dan). JavaScript Contoh-contoh ini menggunakan penyedia kunci master AWS Key Management Service (AWS KMS) atau AWS KMS keyring yang kompatibel.

C

```
// Create an AWS KMS keyring
//   The input is the Amazon Resource Name (ARN)
//   of an AWS KMS key
struct aws_cryptosdk_keyring *kms_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder().Build(kms_key_arn);
```

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x dari CMM AWS Encryption SDK for Java caching kunci data tidak digunakan lagi. Dengan versi 3. x, Anda juga dapat menggunakan keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

```
// Create an AWS KMS master key provider
//   The input is the Amazon Resource Name (ARN)
//   of an AWS KMS key
```

```
MasterKeyProvider<KmsMasterKey> keyProvider =
 KmsMasterKeyProvider.builder().buildStrict(kmsKeyArn);
```

JavaScript Browser

Di browser, Anda harus menyuntikkan kredensyal Anda dengan aman. Contoh ini mendefinisikan kredensyal dalam webpack (kms.webpack.config) yang menyelesaikan kredensyal saat runtime. Ini menciptakan instance penyedia AWS KMS klien dari AWS KMS klien dan kredensialnya. Kemudian, ketika membuat keyring, ia meneruskan penyedia klien ke konstruktor bersama dengan (. AWS KMS key `generatorKeyId`)

```
const { accessKeyId, secretAccessKey, sessionToken } = credentials

const clientProvider = getClient(KMS, {
    credentials: {
      accessKeyId,
      secretAccessKey,
      sessionToken
    }
  })

/*  Create an AWS KMS keyring
 *  You must configure the AWS KMS keyring with at least one AWS KMS key
*  The input is the Amazon Resource Name (ARN)
 */ of an AWS KMS key
const keyring = new KmsKeyringBrowser({
    clientProvider,
    generatorKeyId,
    keyIds,
  })
```

JavaScript Node.js

```
/* Create an AWS KMS keyring
 *   The input is the Amazon Resource Name (ARN)
*/   of an AWS KMS key
const keyring = new KmsKeyringNode({ generatorKeyId })
```

Python

```
# Create an AWS KMS master key provider
```

```
#  The input is the Amazon Resource Name (ARN)
#  of an AWS KMS key
key_provider =
 aws_encryption_sdk.StrictAwsKmsMasterKeyProvider(key_ids=[kms_key_arn])
```

- Buat manajer materi kriptografi caching (caching CMM).

Kaitkan CMM caching Anda dengan cache dan penyedia kunci utama atau keyring Anda. Kemudian, atur ambang keamanan cache pada CMM caching.

C

Di dalam AWS Encryption SDK for C, Anda dapat membuat CMM caching dari CMM yang mendasarinya, seperti CMM default, atau dari keyring. Contoh ini membuat CMM caching dari keyring.

Setelah Anda membuat CMM caching, Anda dapat melepaskan referensi Anda ke keyring dan cache. Lihat perinciannya di the section called “Penghitungan referensi”.

```
// Create the caching CMM
//   Set the partition ID to NULL.
//   Set the required maximum age value to 60 seconds.
struct aws_cryptosdk_cmm *caching_cmm =
 aws_cryptosdk_caching_cmm_new_from_keyring(allocator, cache, kms_keyring, NULL,
 60, AWS_TIMESTAMP_SECS);

// Add an optional message threshold
//   The cached data key will not be used for more than 10 messages.
aws_status = aws_cryptosdk_caching_cmm_set_limit_messages(caching_cmm, 10);

// Release your references to the cache and the keyring.
aws_cryptosdk_materials_cache_release(cache);
aws_cryptosdk_keyring_release(kms_keyring);
```

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x AWS Encryption SDK for Java tidak mendukung caching kunci data, tetapi mendukung keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

```
/*
 * Security thresholds
 *   Max entry age is required.
 *   Max messages (and max bytes) per entry are optional
 */
int MAX_ENTRY_AGE_SECONDS = 60;
int MAX_ENTRY_MSGS = 10;

//Create a caching CMM
CryptoMaterialsManager cachingCmm =
    CachingCryptoMaterialsManager.newBuilder().withMasterKeyProvider(keyProvider)
                                 .withCache(cache)
                                 .withMaxAge(MAX_ENTRY_AGE_SECONDS,
 TimeUnit.SECONDS)
                                 .withMessageUseLimit(MAX_ENTRY_MSGS)
                                 .build();
```

JavaScript Browser

```
/*
 * Security thresholds
 *   Max age (in milliseconds) is required.
 *   Max messages (and max bytes) per entry are optional.
 */
const maxAge = 1000 * 60
const maxMessagesEncrypted = 10

/* Create a caching CMM from a keyring  */
const cachingCmm = new WebCryptoCachingMaterialsManager({
  backingMaterials: keyring,
  cache,
  maxAge,
  maxMessagesEncrypted
})
```

JavaScript Node.js

```
/*
 * Security thresholds
 *   Max age (in milliseconds) is required.
 *   Max messages (and max bytes) per entry are optional.
 */
const maxAge = 1000 * 60
const maxMessagesEncrypted = 10

/* Create a caching CMM from a keyring  */
const cachingCmm = new NodeCachingMaterialsManager({
  backingMaterials: keyring,
  cache,
  maxAge,
  maxMessagesEncrypted
})
```

Python

```
# Security thresholds
#   Max entry age is required.
#   Max messages (and max bytes) per entry are optional
#
MAX_ENTRY_AGE_SECONDS = 60.0
MAX_ENTRY_MESSAGES = 10

# Create a caching CMM
caching_cmm = CachingCryptoMaterialsManager(
    master_key_provider=key_provider,
    cache=cache,
    max_age=MAX_ENTRY_AGE_SECONDS,
    max_messages_encrypted=MAX_ENTRY_MESSAGES
)
```

Hanya itu yang perlu Anda lakukan. Kemudian, biarkan AWS Encryption SDK mengelola cache untuk Anda, atau tambahkan logika manajemen cache Anda sendiri.

Saat Anda ingin menggunakan caching kunci data dalam panggilan untuk mengenkripsi atau mendekripsi data, tentukan CMM caching Anda alih-alih penyedia kunci master atau CMM lainnya.

> **Note**
>
> Jika Anda mengenkripsi aliran data, atau data apa pun dengan ukuran yang tidak diketahui, pastikan untuk menentukan ukuran data dalam permintaan. AWS Encryption SDK Tidak menggunakan caching kunci data saat mengenkripsi data dengan ukuran yang tidak diketahui.

C

Di AWS Encryption SDK for C, Anda membuat sesi dengan CMM caching dan kemudian memproses sesi.

Secara default, ketika ukuran pesan tidak diketahui dan tidak terbatas, kunci data AWS Encryption SDK tidak cache. Untuk mengizinkan caching saat Anda tidak mengetahui ukuran data yang tepat, gunakan `aws_cryptosdk_session_set_message_bound` metode ini untuk mengatur ukuran maksimum pesan. Atur batas lebih besar dari perkiraan ukuran pesan. Jika ukuran pesan sebenarnya melebihi batas, operasi enkripsi gagal.

```
/* Create a session with the caching CMM. Set the session mode to encrypt. */
struct aws_cryptosdk_session *session =
 aws_cryptosdk_session_new_from_cmm_2(allocator, AWS_CRYPTOSDK_ENCRYPT,
 caching_cmm);

/* Set a message bound of 1000 bytes */
aws_status = aws_cryptosdk_session_set_message_bound(session, 1000);

/* Encrypt the message using the session with the caching CMM */
aws_status = aws_cryptosdk_session_process(
             session, output_buffer, output_capacity, &output_produced,
 input_buffer, input_len, &input_consumed);

/* Release your references to the caching CMM and the session. */
aws_cryptosdk_cmm_release(caching_cmm);
aws_cryptosdk_session_destroy(session);
```

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x dari CMM AWS Encryption SDK for Java caching kunci data tidak digunakan lagi. Dengan versi 3. x, Anda juga dapat menggunakan keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

```
// When the call to encryptData specifies a caching CMM,
// the encryption operation uses the data key cache
final AwsCrypto encryptionSdk = AwsCrypto.standard();
return encryptionSdk.encryptData(cachingCmm, plaintext_source).getResult();
```

JavaScript Browser

```
const { result } = await encrypt(cachingCmm, plaintext)
```

JavaScript Node.js

Saat Anda menggunakan CMM caching di AWS Encryption SDK for JavaScript for Node.js, `encrypt` metode ini membutuhkan panjang plaintext. Jika Anda tidak menyediakannya, kunci data tidak di-cache. Jika Anda memberikan panjang, tetapi data plaintext yang Anda berikan melebihi panjang itu, operasi enkripsi gagal. Jika Anda tidak tahu persis panjang plaintext, seperti saat Anda streaming data, berikan nilai yang diharapkan terbesar.

```
const { result } = await encrypt(cachingCmm, plaintext, { plaintextLength:
 plaintext.length })
```

Python

```
# Set up an encryption client
client = aws_encryption_sdk.EncryptionSDKClient()

# When the call to encrypt specifies a caching CMM,
# the encryption operation uses the data key cache
#
encrypted_message, header = client.encrypt(
    source=plaintext_source,
    materials_manager=caching_cmm
)
```

Contoh caching kunci data: Enkripsi string

Contoh kode sederhana ini menggunakan caching kunci data saat mengenkripsi string. Ini menggabungkan kode dari step-by-step prosedur ke kode pengujian yang dapat Anda jalankan.

Contoh ini membuat cache lokal dan penyedia kunci master atau keyring untuk file AWS KMS key. Kemudian, ia menggunakan cache lokal dan penyedia kunci master atau keyring untuk membuat

CMM caching dengan ambang keamanan yang sesuai. Di Java dan Python, permintaan enkripsi menentukan CMM caching, data plaintext untuk mengenkripsi, dan konteks enkripsi. Dalam C, CMM caching ditentukan dalam sesi, dan sesi disediakan untuk permintaan enkripsi.

Untuk menjalankan contoh ini, Anda perlu menyediakan Amazon Resource Name (ARN) dari file. AWS KMS key Pastikan bahwa Anda memiliki izin untuk menggunakan AWS KMS key untuk menghasilkan kunci data.

Untuk contoh dunia nyata yang lebih rinci tentang membuat dan menggunakan cache kunci data, lihatKode contoh caching kunci data.

C

```
/*
 * Copyright 2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License"). You may not use
 * this file except in compliance with the License. A copy of the License is
 * located at
 *
 *     http://aws.amazon.com/apache2.0/
 *
 * or in the "license" file accompanying this file. This file is distributed on an
 * "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
 * implied. See the License for the specific language governing permissions and
 * limitations under the License.
 */

#include <aws/cryptosdk/cache.h>
#include <aws/cryptosdk/cpp/kms_keyring.h>
#include <aws/cryptosdk/session.h>

void encrypt_with_caching(
    uint8_t *ciphertext,     // output will go here (assumes ciphertext_capacity
 bytes already allocated)
    size_t *ciphertext_len,  // length of output will go here
    size_t ciphertext_capacity,
    const char *kms_key_arn,
    int max_entry_age,
    int cache_capacity) {
    const uint64_t MAX_ENTRY_MSGS = 100;

    struct aws_allocator *allocator = aws_default_allocator();
```

```
   // Load error strings for debugging
   aws_cryptosdk_load_error_strings();

   // Create a keyring
   struct aws_cryptosdk_keyring *kms_keyring =
Aws::Cryptosdk::KmsKeyring::Builder().Build(kms_key_arn);

   // Create a cache
   struct aws_cryptosdk_materials_cache *cache =
aws_cryptosdk_materials_cache_local_new(allocator, cache_capacity);

   // Create a caching CMM
   struct aws_cryptosdk_cmm *caching_cmm =
aws_cryptosdk_caching_cmm_new_from_keyring(
       allocator, cache, kms_keyring, NULL, max_entry_age, AWS_TIMESTAMP_SECS);
   if (!caching_cmm) abort();

   if (aws_cryptosdk_caching_cmm_set_limit_messages(caching_cmm, MAX_ENTRY_MSGS))
abort();

   // Create a session
   struct aws_cryptosdk_session *session =
       aws_cryptosdk_session_new_from_cmm_2(allocator, AWS_CRYPTOSDK_ENCRYPT,
caching_cmm);
   if (!session) abort();

   // Encryption context
   struct aws_hash_table *enc_ctx =
aws_cryptosdk_session_get_enc_ctx_ptr_mut(session);
   if (!enc_ctx) abort();
   AWS_STATIC_STRING_FROM_LITERAL(enc_ctx_key, "purpose");
   AWS_STATIC_STRING_FROM_LITERAL(enc_ctx_value, "test");
   if (aws_hash_table_put(enc_ctx, enc_ctx_key, (void *)enc_ctx_value, NULL))
abort();

   // Plaintext data to be encrypted
   const char *my_data = "My plaintext data";
   size_t my_data_len  = strlen(my_data);
   if (aws_cryptosdk_session_set_message_size(session, my_data_len)) abort();

   // When the session uses a caching CMM, the encryption operation uses the data
key cache
   // specified in the caching CMM.
```

```
    size_t bytes_read;
    if (aws_cryptosdk_session_process(
            session,
            ciphertext,
            ciphertext_capacity,
            ciphertext_len,
            (const uint8_t *)my_data,
            my_data_len,
            &bytes_read))
        abort();
    if (!aws_cryptosdk_session_is_done(session) || bytes_read != my_data_len)
 abort();

    aws_cryptosdk_session_destroy(session);
    aws_cryptosdk_cmm_release(caching_cmm);
    aws_cryptosdk_materials_cache_release(cache);
    aws_cryptosdk_keyring_release(kms_keyring);
}
```

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x dari CMM AWS Encryption SDK for Java caching kunci data tidak digunakan lagi. Dengan versi 3. x, Anda juga dapat menggunakan keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

```
// Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

package com.amazonaws.crypto.examples;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoMaterialsManager;
import com.amazonaws.encryptionsdk.MasterKeyProvider;
import com.amazonaws.encryptionsdk.caching.CachingCryptoMaterialsManager;
import com.amazonaws.encryptionsdk.caching.CryptoMaterialsCache;
import com.amazonaws.encryptionsdk.caching.LocalCryptoMaterialsCache;
import com.amazonaws.encryptionsdk.kmssdkv2.KmsMasterKey;
import com.amazonaws.encryptionsdk.kmssdkv2.KmsMasterKeyProvider;
import java.nio.charset.StandardCharsets;
import java.util.Collections;
import java.util.Map;
import java.util.concurrent.TimeUnit;
```

```
/**
 * <p>
 * Encrypts a string using an &KMS; key and data key caching
 *
 * <p>
 * Arguments:
 * <ol>
 * <li>KMS Key ARN: To find the Amazon Resource Name of your &KMS; key,
 *     see 'Find the key ID and ARN' at https://docs.aws.amazon.com/kms/latest/
developerguide/find-cmk-id-arn.html
 * <li>Max entry age: Maximum time (in seconds) that a cached entry can be used
 * <li>Cache capacity: Maximum number of entries in the cache
 * </ol>
 */
public class SimpleDataKeyCachingExample {

    /*
     * Security thresholds
     *   Max entry age is required.
     *   Max messages (and max bytes) per data key are optional
     */
    private static final int MAX_ENTRY_MSGS = 100;

    public static byte[] encryptWithCaching(String kmsKeyArn, int maxEntryAge, int
 cacheCapacity) {
        // Plaintext data to be encrypted
        byte[] myData = "My plaintext data".getBytes(StandardCharsets.UTF_8);

        // Encryption context
        // Most encrypted data should have an associated encryption context
        // to protect integrity. This sample uses placeholder values.
        // For more information see:
        // blogs.aws.amazon.com/security/post/Tx2LZ6WBJJANTNW/How-to-Protect-the-
Integrity-of-Your-Encrypted-Data-by-Using-AWS-Key-Management
        final Map<String, String> encryptionContext =
 Collections.singletonMap("purpose", "test");

        // Create a master key provider
        MasterKeyProvider<KmsMasterKey> keyProvider =
 KmsMasterKeyProvider.builder()
            .buildStrict(kmsKeyArn);

        // Create a cache
        CryptoMaterialsCache cache = new LocalCryptoMaterialsCache(cacheCapacity);
```

```
        // Create a caching CMM
        CryptoMaterialsManager cachingCmm =

 CachingCryptoMaterialsManager.newBuilder().withMasterKeyProvider(keyProvider)
                .withCache(cache)
                .withMaxAge(maxEntryAge, TimeUnit.SECONDS)
                .withMessageUseLimit(MAX_ENTRY_MSGS)
                .build();

        // When the call to encryptData specifies a caching CMM,
        // the encryption operation uses the data key cache
        final AwsCrypto encryptionSdk = AwsCrypto.standard();
        return encryptionSdk.encryptData(cachingCmm, myData,
 encryptionContext).getResult();
    }
}
```

JavaScript Browser

```
// Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

/* This is a simple example of using a caching CMM with a KMS keyring
 * to encrypt and decrypt using the AWS Encryption SDK for Javascript in a browser.
 */

import {
  KmsKeyringBrowser,
  KMS,
  getClient,
  buildClient,
  CommitmentPolicy,
  WebCryptoCachingMaterialsManager,
  getLocalCryptographicMaterialsCache,
} from '@aws-crypto/client-browser'
import { toBase64 } from '@aws-sdk/util-base64-browser'

/* This builds the client with the REQUIRE_ENCRYPT_REQUIRE_DECRYPT commitment
 policy,
 * which enforces that this client only encrypts using committing algorithm suites
 * and enforces that this client
 * will only decrypt encrypted messages
```

```
 * that were created with a committing algorithm suite.
 * This is the default commitment policy
 * if you build the client with `buildClient()`.
 */
const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

/* This is injected by webpack.
 * The webpack.DefinePlugin or @aws-sdk/karma-credential-loader will replace the
 values when bundling.
 * The credential values are pulled from @aws-sdk/credential-provider-node
 * Use any method you like to get credentials into the browser.
 * See kms.webpack.config
 */
declare const credentials: {
  accessKeyId: string
  secretAccessKey: string
  sessionToken: string
}

/* This is done to facilitate testing. */
export async function testCachingCMMExample() {
  /* This example uses an &KMS; keyring. The generator key in a &KMS; keyring
 generates and encrypts the data key.
   * The caller needs kms:GenerateDataKey permission on the &KMS; key in
 generatorKeyId.
   */
  const generatorKeyId =
    'arn:aws:kms:us-west-2:658956600833:alias/EncryptDecrypt'

  /* Adding additional KMS keys that can decrypt.
   * The caller must have kms:Encrypt permission for every &KMS; key in keyIds.
   * You might list several keys in different AWS Regions.
   * This allows you to decrypt the data in any of the represented Regions.
   * In this example, the generator key
   * and the additional key are actually the same &KMS; key.
   * In `generatorId`, this &KMS; key is identified by its alias ARN.
   * In `keyIds`, this &KMS; key is identified by its key ARN.
   * In practice, you would specify different &KMS; keys,
   * or omit the `keyIds` parameter.
   * This is *only* to demonstrate how the &KMS; key ARNs are configured.
   */
  const keyIds = [
```

```
    'arn:aws:kms:us-west-2:658956600833:key/b3537ef1-d8dc-4780-9f5a-55776cbb2f7f',
 ]

 /* Need a client provider that will inject correct credentials.
  * The credentials here are injected by webpack from your environment bundle is
created
  * The credential values are pulled using @aws-sdk/credential-provider-node.
  * See kms.webpack.config
  * You should inject your credential into the browser in a secure manner
  * that works with your application.
  */
 const { accessKeyId, secretAccessKey, sessionToken } = credentials

 /* getClient takes a KMS client constructor
  * and optional configuration values.
  * The credentials can be injected here,
  * because browsers do not have a standard credential discovery process the way
Node.js does.
  */
 const clientProvider = getClient(KMS, {
   credentials: {
     accessKeyId,
     secretAccessKey,
     sessionToken,
   },
 })

 /* You must configure the KMS keyring with your &KMS; keys */
 const keyring = new KmsKeyringBrowser({
   clientProvider,
   generatorKeyId,
   keyIds,
 })

 /* Create a cache to hold the data keys (and related cryptographic material).
  * This example uses the local cache provided by the Encryption SDK.
  * The `capacity` value represents the maximum number of entries
  * that the cache can hold.
  * To make room for an additional entry,
  * the cache evicts the oldest cached entry.
  * Both encrypt and decrypt requests count independently towards this threshold.
  * Entries that exceed any cache threshold are actively removed from the cache.
  * By default, the SDK checks one item in the cache every 60 seconds (60,000
milliseconds).
```

```
  * To change this frequency, pass in a `proactiveFrequency` value
  * as the second parameter. This value is in milliseconds.
  */
 const capacity = 100
 const cache = getLocalCryptographicMaterialsCache(capacity)

 /* The partition name lets multiple caching CMMs share the same local
cryptographic cache.
  * By default, the entries for each CMM are cached separately. However, if you
want these CMMs to share the cache,
  * use the same partition name for both caching CMMs.
  * If you don't supply a partition name, the Encryption SDK generates a random
name for each caching CMM.
  * As a result, sharing elements in the cache MUST be an intentional operation.
  */
 const partition = 'local partition name'

 /* maxAge is the time in milliseconds that an entry will be cached.
  * Elements are actively removed from the cache.
  */
 const maxAge = 1000 * 60

 /* The maximum number of bytes that will be encrypted under a single data key.
  * This value is optional,
  * but you should configure the lowest practical value.
  */
 const maxBytesEncrypted = 100

 /* The maximum number of messages that will be encrypted under a single data key.
  * This value is optional,
  * but you should configure the lowest practical value.
  */
 const maxMessagesEncrypted = 10

 const cachingCMM = new WebCryptoCachingMaterialsManager({
   backingMaterials: keyring,
   cache,
   partition,
   maxAge,
   maxBytesEncrypted,
   maxMessagesEncrypted,
 })

 /* Encryption context is a *very* powerful tool for controlling
```

```
   * and managing access.
   * When you pass an encryption context to the encrypt function,
   * the encryption context is cryptographically bound to the ciphertext.
   * If you don't pass in the same encryption context when decrypting,
   * the decrypt function fails.
   * The encryption context is ***not*** secret!
   * Encrypted data is opaque.
   * You can use an encryption context to assert things about the encrypted data.
   * The encryption context helps you to determine
   * whether the ciphertext you retrieved is the ciphertext you expect to decrypt.
   * For example, if you are are only expecting data from 'us-west-2',
   * the appearance of a different AWS Region in the encryption context can indicate
 malicious interference.
   * See: https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/
concepts.html#encryption-context
   *
   * Also, cached data keys are reused ***only*** when the encryption contexts
 passed into the functions are an exact case-sensitive match.
   * See: https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-
caching-details.html#caching-encryption-context
   */
  const encryptionContext = {
    stage: 'demo',
    purpose: 'simple demonstration app',
    origin: 'us-west-2',
  }

  /* Find data to encrypt. */
  const plainText = new Uint8Array([1, 2, 3, 4, 5])

  /* Encrypt the data.
   * The caching CMM only reuses data keys
   * when it know the length (or an estimate) of the plaintext.
   * However, in the browser,
   * you must provide all of the plaintext to the encrypt function.
   * Therefore, the encrypt function in the browser knows the length of the
 plaintext
   * and does not accept a plaintextLength option.
   */
  const { result } = await encrypt(cachingCMM, plainText, { encryptionContext })

  /* Log the plain text
   * only for testing and to show that it works.
   */
```

```
 console.log('plainText:', plainText)
 document.write('</br>plainText:' + plainText + '</br>')

 /* Log the base64-encoded result
  * so that you can try decrypting it with another AWS Encryption SDK
implementation.
  */
 const resultBase64 = toBase64(result)
 console.log(resultBase64)
 document.write(resultBase64)

 /* Decrypt the data.
  * NOTE: This decrypt request will not use the data key
  * that was cached during the encrypt operation.
  * Data keys for encrypt and decrypt operations are cached separately.
  */
 const { plaintext, messageHeader } = await decrypt(cachingCMM, result)

 /* Grab the encryption context so you can verify it. */
 const { encryptionContext: decryptedContext } = messageHeader

 /* Verify the encryption context.
  * If you use an algorithm suite with signing,
  * the Encryption SDK adds a name-value pair to the encryption context that
contains the public key.
  * Because the encryption context might contain additional key-value pairs,
  * do not include a test that requires that all key-value pairs match.
  * Instead, verify that the key-value pairs that you supplied to the `encrypt`
function are included in the encryption context that the `decrypt` function
returns.
  */
 Object.entries(encryptionContext).forEach(([key, value]) => {
   if (decryptedContext[key] !== value)
     throw new Error('Encryption Context does not match expected values')
 })

 /* Log the clear message
  * only for testing and to show that it works.
  */
 document.write('</br>Decrypted:' + plaintext)
 console.log(plaintext)

 /* Return the values to make testing easy. */
 return { plainText, plaintext }
```

```
}
```

JavaScript Node.js

```
// Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

import {
  KmsKeyringNode,
  buildClient,
  CommitmentPolicy,
  NodeCachingMaterialsManager,
  getLocalCryptographicMaterialsCache,
} from '@aws-crypto/client-node'

/* This builds the client with the REQUIRE_ENCRYPT_REQUIRE_DECRYPT commitment
 policy,
 * which enforces that this client only encrypts using committing algorithm suites
 * and enforces that this client
 * will only decrypt encrypted messages
 * that were created with a committing algorithm suite.
 * This is the default commitment policy
 * if you build the client with `buildClient()`.
 */
const { encrypt, decrypt } = buildClient(
  CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT
)

export async function cachingCMMNodeSimpleTest() {
  /* An &KMS; key is required to generate the data key.
   * You need kms:GenerateDataKey permission on the &KMS; key in generatorKeyId.
   */
  const generatorKeyId =
    'arn:aws:kms:us-west-2:658956600833:alias/EncryptDecrypt'

  /* Adding alternate &KMS; keys that can decrypt.
   * Access to kms:Encrypt is required for every &KMS; key in keyIds.
   * You might list several keys in different AWS Regions.
   * This allows you to decrypt the data in any of the represented Regions.
   * In this example, the generator key
   * and the additional key are actually the same &KMS; key.
   * In `generatorId`, this &KMS; key is identified by its alias ARN.
   * In `keyIds`, this &KMS; key is identified by its key ARN.
```

```
   * In practice, you would specify different &KMS; keys,
   * or omit the `keyIds` parameter.
   * This is *only* to demonstrate how the &KMS; key ARNs are configured.
   */
  const keyIds = [
    'arn:aws:kms:us-west-2:658956600833:key/b3537ef1-d8dc-4780-9f5a-55776cbb2f7f',
  ]

  /* The &KMS; keyring must be configured with the desired &KMS; keys
   * This example passes the keyring to the caching CMM
   * instead of using it directly.
   */
  const keyring = new KmsKeyringNode({ generatorKeyId, keyIds })

  /* Create a cache to hold the data keys (and related cryptographic material).
   * This example uses the local cache provided by the Encryption SDK.
   * The `capacity` value represents the maximum number of entries
   * that the cache can hold.
   * To make room for an additional entry,
   * the cache evicts the oldest cached entry.
   * Both encrypt and decrypt requests count independently towards this threshold.
   * Entries that exceed any cache threshold are actively removed from the cache.
   * By default, the SDK checks one item in the cache every 60 seconds (60,000
milliseconds).
   * To change this frequency, pass in a `proactiveFrequency` value
   * as the second parameter. This value is in milliseconds.
   */
  const capacity = 100
  const cache = getLocalCryptographicMaterialsCache(capacity)

  /* The partition name lets multiple caching CMMs share the same local
cryptographic cache.
   * By default, the entries for each CMM are cached separately. However, if you
want these CMMs to share the cache,
   * use the same partition name for both caching CMMs.
   * If you don't supply a partition name, the Encryption SDK generates a random
name for each caching CMM.
   * As a result, sharing elements in the cache MUST be an intentional operation.
   */
  const partition = 'local partition name'

  /* maxAge is the time in milliseconds that an entry will be cached.
   * Elements are actively removed from the cache.
   */
```

```
  const maxAge = 1000 * 60

  /* The maximum amount of bytes that will be encrypted under a single data key.
   * This value is optional,
   * but you should configure the lowest value possible.
   */
  const maxBytesEncrypted = 100

  /* The maximum number of messages that will be encrypted under a single data key.
   * This value is optional,
   * but you should configure the lowest value possible.
   */
  const maxMessagesEncrypted = 10

  const cachingCMM = new NodeCachingMaterialsManager({
    backingMaterials: keyring,
    cache,
    partition,
    maxAge,
    maxBytesEncrypted,
    maxMessagesEncrypted,
  })

  /* Encryption context is a *very* powerful tool for controlling
   * and managing access.
   * When you pass an encryption context to the encrypt function,
   * the encryption context is cryptographically bound to the ciphertext.
   * If you don't pass in the same encryption context when decrypting,
   * the decrypt function fails.
   * The encryption context is ***not*** secret!
   * Encrypted data is opaque.
   * You can use an encryption context to assert things about the encrypted data.
   * The encryption context helps you to determine
   * whether the ciphertext you retrieved is the ciphertext you expect to decrypt.
   * For example, if you are are only expecting data from 'us-west-2',
   * the appearance of a different AWS Region in the encryption context can indicate
 malicious interference.
   * See: https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/
concepts.html#encryption-context
   *
   * Also, cached data keys are reused ***only*** when the encryption contexts
 passed into the functions are an exact case-sensitive match.
   * See: https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-
caching-details.html#caching-encryption-context
```

```
   */
  const encryptionContext = {
    stage: 'demo',
    purpose: 'simple demonstration app',
    origin: 'us-west-2',
  }

  /* Find data to encrypt.  A simple string. */
  const cleartext = 'asdf'

  /* Encrypt the data.
   * The caching CMM only reuses data keys
   * when it know the length (or an estimate) of the plaintext.
   * If you do not know the length,
   * because the data is a stream
   * provide an estimate of the largest expected value.
   *
   * If your estimate is smaller than the actual plaintext length
   * the AWS Encryption SDK will throw an exception.
   *
   * If the plaintext is not a stream,
   * the AWS Encryption SDK uses the actual plaintext length
   * instead of any length you provide.
   */
  const { result } = await encrypt(cachingCMM, cleartext, {
    encryptionContext,
    plaintextLength: 4,
  })

  /* Decrypt the data.
   * NOTE: This decrypt request will not use the data key
   * that was cached during the encrypt operation.
   * Data keys for encrypt and decrypt operations are cached separately.
   */
  const { plaintext, messageHeader } = await decrypt(cachingCMM, result)

  /* Grab the encryption context so you can verify it. */
  const { encryptionContext: decryptedContext } = messageHeader

  /* Verify the encryption context.
   * If you use an algorithm suite with signing,
   * the Encryption SDK adds a name-value pair to the encryption context that
 contains the public key.
   * Because the encryption context might contain additional key-value pairs,
```

```
   * do not include a test that requires that all key-value pairs match.
   * Instead, verify that the key-value pairs that you supplied to the `encrypt`
 function are included in the encryption context that the `decrypt` function
 returns.
   */
  Object.entries(encryptionContext).forEach(([key, value]) => {
    if (decryptedContext[key] !== value)
      throw new Error('Encryption Context does not match expected values')
  })

  /* Return the values so the code can be tested. */
  return { plaintext, result, cleartext, messageHeader }
}
```

Python

```
# Copyright 2017 Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the "License"). You
# may not use this file except in compliance with the License. A copy of
# the License is located at
#
# http://aws.amazon.com/apache2.0/
#
# or in the "license" file accompanying this file. This file is
# distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF
# ANY KIND, either express or implied. See the License for the specific
# language governing permissions and limitations under the License.
"""Example of encryption with data key caching."""
import aws_encryption_sdk
from aws_encryption_sdk import CommitmentPolicy


def encrypt_with_caching(kms_key_arn, max_age_in_cache, cache_capacity):
    """Encrypts a string using an &KMS; key and data key caching.

    :param str kms_key_arn: Amazon Resource Name (ARN) of the &KMS; key
    :param float max_age_in_cache: Maximum time in seconds that a cached entry can
 be used
    :param int cache_capacity: Maximum number of entries to retain in cache at once
    """
    # Data to be encrypted
    my_data = "My plaintext data"
```

```
   # Security thresholds
   #   Max messages (or max bytes per) data key are optional
   MAX_ENTRY_MESSAGES = 100

   # Create an encryption context
   encryption_context = {"purpose": "test"}

   # Set up an encryption client with an explicit commitment policy. Note that if
you do not explicitly choose a
   # commitment policy, REQUIRE_ENCRYPT_REQUIRE_DECRYPT is used by default.
   client =
aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.REQUIRE_ENCRYPT_R

   # Create a master key provider for the &KMS; key
   key_provider =
aws_encryption_sdk.StrictAwsKmsMasterKeyProvider(key_ids=[kms_key_arn])

   # Create a local cache
   cache = aws_encryption_sdk.LocalCryptoMaterialsCache(cache_capacity)

   # Create a caching CMM
   caching_cmm = aws_encryption_sdk.CachingCryptoMaterialsManager(
       master_key_provider=key_provider,
       cache=cache,
       max_age=max_age_in_cache,
       max_messages_encrypted=MAX_ENTRY_MESSAGES,
   )

   # When the call to encrypt data specifies a caching CMM,
   # the encryption operation uses the data key cache specified
   # in the caching CMM
   encrypted_message, _header = client.encrypt(
       source=my_data, materials_manager=caching_cmm,
encryption_context=encryption_context
   )

   return encrypted_message
```

Mengatur ambang keamanan cache

Saat Anda menerapkan caching kunci data, Anda perlu mengonfigurasi ambang keamanan yang diberlakukan CMM caching.

Ambang batas keamanan membantu Anda membatasi berapa lama setiap kunci data yang di-cache digunakan dan berapa banyak data yang dilindungi di bawah setiap kunci data. CMM caching mengembalikan kunci data cache hanya ketika entri cache sesuai dengan semua ambang keamanan. Jika entri cache melebihi ambang batas apa pun, entri tidak digunakan untuk operasi saat ini dan dikeluarkan dari cache sesegera mungkin. Penggunaan pertama setiap kunci data (sebelum caching) dikecualikan dari ambang batas ini.

Sebagai aturan, gunakan jumlah minimum caching yang diperlukan untuk memenuhi tujuan biaya dan kinerja Anda.

AWS Encryption SDK Satu-satunya cache kunci data yang dienkripsi dengan menggunakan fungsi derivasi kunci. Juga, ini menetapkan batas atas untuk beberapa nilai ambang batas. Pembatasan ini memastikan bahwa kunci data tidak digunakan kembali di luar batas kriptografinya. Namun, karena kunci data plaintext Anda di-cache (dalam memori, secara default), cobalah untuk meminimalkan waktu penyimpanan kunci. Juga, cobalah untuk membatasi data yang mungkin terekspos jika kunci dikompromikan.

Untuk contoh pengaturan ambang keamanan cache, lihat AWS Encryption SDK: Cara Memutuskan apakah Caching Kunci Data Tepat untuk Aplikasi Anda di Blog Keamanan. AWS

> **Note**
>
> CMM caching memberlakukan semua ambang batas berikut. Jika Anda tidak menentukan nilai opsional, CMM caching menggunakan nilai default.
> Untuk menonaktifkan caching kunci data sementara, implementasi Java dan Python menyediakan cache materi kriptografi null (cache null). AWS Encryption SDK Cache null mengembalikan miss untuk setiap `GET` permintaan dan tidak menanggapi `PUT` permintaan. Kami menyarankan Anda menggunakan cache null alih-alih mengatur kapasitas cache atau ambang keamanan ke 0. Untuk informasi selengkapnya, lihat cache null di Java dan Python.

Usia maksimal (wajib)

Menentukan berapa lama entri cache dapat digunakan, dimulai saat ditambahkan. Nilai ini diperlukan. Masukkan nilai yang lebih besar dari 0. AWS Encryption SDK Itu tidak membatasi nilai usia maksimum.

Semua implementasi bahasa AWS Encryption SDK menentukan usia maksimum dalam hitungan detik, kecuali untuk AWS Encryption SDK for JavaScript, yang menggunakan milidetik.

Gunakan interval terpendek yang masih memungkinkan aplikasi Anda mendapat manfaat dari cache. Anda dapat menggunakan ambang batas usia maksimum seperti kebijakan rotasi kunci. Gunakan untuk membatasi penggunaan kembali kunci data, meminimalkan paparan materi kriptografi, dan mengusir kunci data yang kebijakannya mungkin telah berubah saat di-cache.

Pesan maksimum dienkripsi (opsional)

Menentukan jumlah maksimum pesan yang kunci data cache dapat mengenkripsi. Nilai ini bersifat opsional. Masukkan nilai antara 1 dan 2 ^ 32 pesan. Nilai default adalah 2 ^ 32 pesan.

Setel jumlah pesan yang dilindungi oleh setiap kunci cache menjadi cukup besar untuk mendapatkan nilai dari penggunaan kembali, tetapi cukup kecil untuk membatasi jumlah pesan yang mungkin terpapar jika kunci dikompromikan.

Byte maksimum dienkripsi (opsional)

Menentukan jumlah maksimum byte yang kunci data cache dapat mengenkripsi. Nilai ini bersifat opsional. Masukkan nilai antara 0 dan 2 ^ 63 - 1. Nilai default adalah 2 ^ 63 - 1. Nilai 0 memungkinkan Anda menggunakan caching kunci data hanya ketika Anda mengenkripsi string pesan kosong.

Byte dalam permintaan saat ini disertakan saat mengevaluasi ambang batas ini. Jika byte yang diproses, ditambah byte saat ini, melebihi ambang batas, kunci data yang di-cache dikeluarkan dari cache, meskipun mungkin telah digunakan pada permintaan yang lebih kecil.

Detail caching kunci data

Sebagian besar aplikasi dapat menggunakan implementasi default caching kunci data tanpa menulis kode kustom. Bagian ini menjelaskan implementasi default dan beberapa detail tentang opsi.

Topik

Cara kerja caching kunci data

Saat Anda menggunakan caching kunci data dalam permintaan untuk mengenkripsi atau mendekripsi data, yang AWS Encryption SDK pertama akan mencari cache untuk kunci data yang cocok dengan permintaan. Jika menemukan kecocokan yang valid, ia menggunakan kunci data cache untuk mengenkripsi data. Jika tidak, itu menghasilkan kunci data baru, seperti halnya tanpa cache.

Caching kunci data tidak digunakan untuk data dengan ukuran yang tidak diketahui, seperti data yang dialirkan. Hal ini memungkinkan CMM caching untuk menerapkan ambang batas byte maksimum dengan benar. Untuk menghindari perilaku ini, tambahkan ukuran pesan ke permintaan enkripsi.

Selain cache, caching kunci data menggunakan pengelola bahan kriptografi caching (caching CMM). CMM caching adalah manajer bahan kriptografi khusus (CMM) yang berinteraksi dengan cache dan CMM yang mendasarinya. (Saat Anda menentukan penyedia kunci master atau keyring, CMM AWS Encryption SDK default akan dibuat untuk Anda.) CMM caching menyimpan kunci data yang dikembalikan oleh CMM yang mendasarinya. CMM caching juga memberlakukan ambang keamanan cache yang Anda tetapkan.

Untuk mencegah kunci data yang salah dipilih dari cache, semua caching yang kompatibel CMMs mengharuskan properti berikut dari bahan kriptografi yang di-cache cocok dengan permintaan bahan.

- Suite algoritma
- Konteks enkripsi (bahkan saat kosong)
- Nama partisi (string yang mengidentifikasi CMM caching)
- (Hanya dekripsi) Kunci data terenkripsi

> **Note**
>
> Kunci data AWS Encryption SDK cache hanya ketika rangkaian algoritma menggunakan fungsi derivasi kunci.

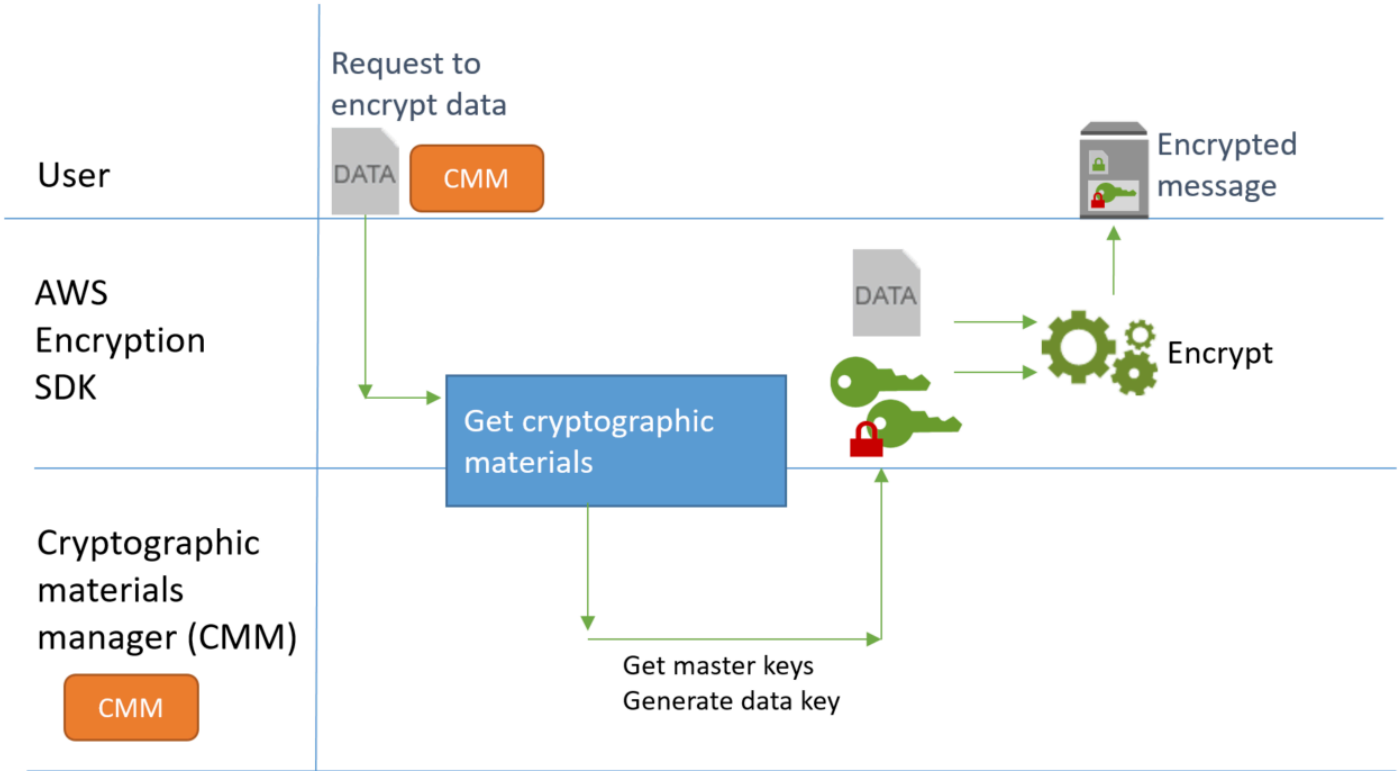
Alur kerja berikut menunjukkan bagaimana permintaan untuk mengenkripsi data diproses dengan dan tanpa caching kunci data. Mereka menunjukkan bagaimana komponen caching yang Anda buat, termasuk cache dan CMM caching, digunakan dalam proses.

Enkripsi data tanpa caching

Untuk mendapatkan materi enkripsi tanpa caching:

1. Aplikasi meminta AWS Encryption SDK untuk mengenkripsi data.

   Permintaan menentukan penyedia kunci master atau keyring. AWS Encryption SDK Membuat CMM default yang berinteraksi dengan penyedia kunci master atau keyring Anda.
2. Mereka AWS Encryption SDK meminta CMM untuk bahan enkripsi (dapatkan bahan kriptografi).
3. CMM meminta keyring (C dan JavaScript) atau penyedia kunci master (Java dan Python) untuk materi kriptografi. Ini mungkin melibatkan panggilan ke layanan kriptografi, seperti AWS Key Management Service (AWS KMS). CMM mengembalikan materi enkripsi ke file. AWS Encryption SDK
4. AWS Encryption SDK Menggunakan kunci data plaintext untuk mengenkripsi data. Ini menyimpan data terenkripsi dan kunci data terenkripsi dalam pesan terenkripsi, yang dikembalikan ke pengguna.



Enkripsi data dengan caching

Untuk mendapatkan materi enkripsi dengan caching kunci data:

1. Aplikasi meminta AWS Encryption SDK untuk mengenkripsi data.

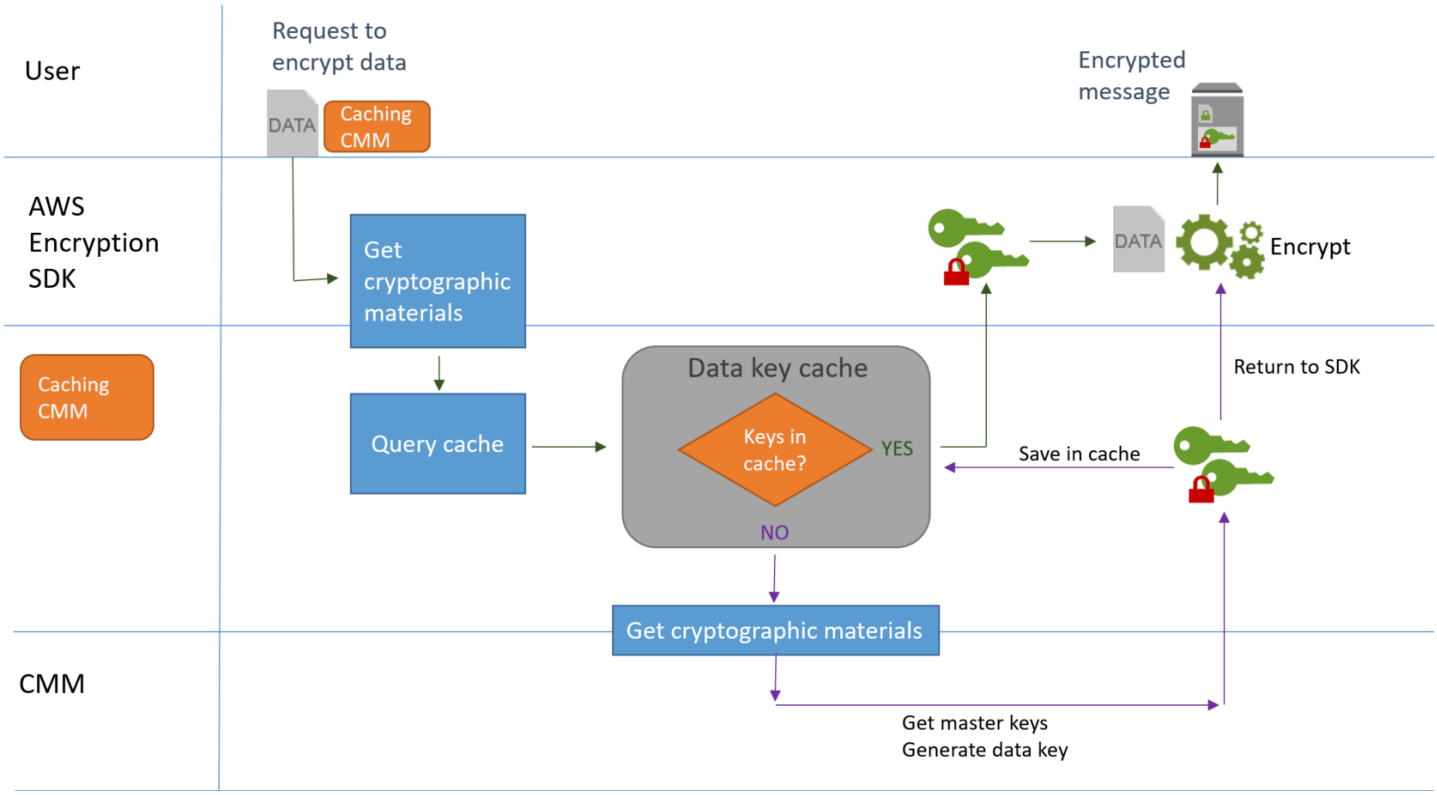
   Permintaan tersebut menentukan manajer bahan kriptografi caching (caching CMM) yang terkait dengan manajer bahan kriptografi yang mendasarinya (CMM). Saat Anda menentukan penyedia kunci master atau keyring, CMM AWS Encryption SDK default akan dibuat untuk Anda.
2. SDK meminta CMM caching yang ditentukan untuk materi enkripsi.
3. CMM caching meminta materi enkripsi dari cache.
   a. Jika cache menemukan kecocokan, cache akan memperbarui usia dan menggunakan nilai entri cache yang cocok, dan mengembalikan materi enkripsi yang di-cache ke CMM caching.

      Jika entri cache sesuai dengan ambang keamanannya, CMM caching mengembalikannya ke SDK. Jika tidak, ia memberitahu cache untuk mengusir entri dan melanjutkan seolah-olah tidak ada kecocokan.
   b. Jika cache tidak dapat menemukan kecocokan yang valid, CMM caching meminta CMM yang mendasarinya untuk menghasilkan kunci data baru.

CMM yang mendasarinya mendapatkan materi kriptografi dari keyring (C dan JavaScript) atau penyedia kunci master (Java dan Python). Ini mungkin melibatkan panggilan ke layanan, seperti AWS Key Management Service. CMM yang mendasari mengembalikan plaintext dan salinan terenkripsi dari kunci data ke CMM caching.

CMM caching menyimpan materi enkripsi baru dalam cache.

4. CMM caching mengembalikan materi enkripsi ke file. AWS Encryption SDK
5. AWS Encryption SDK Menggunakan kunci data plaintext untuk mengenkripsi data. Ini menyimpan data terenkripsi dan kunci data terenkripsi dalam pesan terenkripsi, yang dikembalikan ke pengguna.



Membuat cache bahan kriptografi

AWS Encryption SDK Mendefinisikan persyaratan untuk cache bahan kriptografi yang digunakan dalam caching kunci data. Ini juga menyediakan cache lokal, yang merupakan cache yang dapat dikonfigurasi, dalam memori, yang paling jarang digunakan (LRU). Untuk membuat instance cache lokal, gunakan `LocalCryptoMaterialsCache` konstruktor di Java dan Python, fungsi JavaScript

di, getLocalCryptographic MaterialsCache atau `aws_cryptosdk_materials_cache_local_new` konstruktor di C.

Cache lokal mencakup logika untuk manajemen cache dasar, termasuk menambahkan, mengusir, dan mencocokkan entri cache, dan memelihara cache. Anda tidak perlu menulis logika manajemen cache khusus apa pun. Anda dapat menggunakan cache lokal apa adanya, menyesuaikannya, atau mengganti cache yang kompatibel.

Saat Anda membuat cache lokal, Anda mengatur kapasitasnya, yaitu jumlah entri maksimum yang dapat disimpan cache. Pengaturan ini membantu Anda merancang cache yang efisien dengan penggunaan kembali kunci data terbatas.

The AWS Encryption SDK for Java and the AWS Encryption SDK for Python juga menyediakan cache materi kriptografi null ()NullCryptoMaterialsCache. NullCryptoMaterialsCache Pengembalian kehilangan untuk semua `GET` operasi dan tidak menanggapi `PUT` operasi. Anda dapat menggunakan NullCryptoMaterialsCache dalam pengujian atau untuk menonaktifkan sementara caching dalam aplikasi yang menyertakan kode caching.

Dalam AWS Encryption SDK, setiap cache materi kriptografi dikaitkan dengan manajer bahan kriptografi caching (caching CMM). CMM caching mendapatkan kunci data dari cache, menempatkan kunci data dalam cache, dan memberlakukan ambang keamanan yang Anda tetapkan. Saat Anda membuat CMM caching, Anda menentukan cache yang digunakannya dan CMM atau penyedia kunci master yang mendasarinya yang menghasilkan kunci data yang di-cache.

Membuat manajer materi kriptografi caching

Untuk mengaktifkan caching kunci data, Anda membuat cache dan pengelola materi kriptografi caching (caching CMM). Kemudian, dalam permintaan Anda untuk mengenkripsi atau mendekripsi data, Anda menentukan CMM caching, bukan manajer bahan kriptografi standar (CMM), atau penyedia kunci master atau keyring.

Ada dua jenis CMMs. Keduanya mendapatkan kunci data (dan materi kriptografi terkait), tetapi dengan cara yang berbeda, sebagai berikut:

- CMM dikaitkan dengan keyring (C atau JavaScript) atau penyedia kunci master (Java dan Python). Ketika SDK meminta CMM untuk bahan enkripsi atau dekripsi, CMM mendapatkan materi dari keyring atau penyedia kunci masternya. Di Java dan Python, CMM menggunakan kunci master untuk menghasilkan, mengenkripsi, atau mendekripsi kunci data. Dalam C dan JavaScript, keyring menghasilkan, mengenkripsi, dan mengembalikan materi kriptografi.

- CMM caching dikaitkan dengan satu cache, seperti cache lokal, dan CMM yang mendasarinya. Ketika SDK meminta CMM caching untuk materi kriptografi, CMM caching mencoba untuk mendapatkannya dari cache. Jika tidak dapat menemukan kecocokan, CMM caching menanyakan CMM yang mendasarinya untuk materi. Kemudian, ia menyimpan materi kriptografi baru sebelum mengembalikannya ke penelepon.

CMM caching juga memberlakukan ambang keamanan yang Anda tetapkan untuk setiap entri cache. Karena ambang keamanan diatur dan diberlakukan oleh CMM caching, Anda dapat menggunakan cache yang kompatibel, bahkan jika cache tidak dirancang untuk materi sensitif.

Apa yang ada dalam entri cache kunci data?

Caching kunci data menyimpan kunci data dan materi kriptografi terkait dalam cache. Setiap entri mencakup elemen-elemen yang tercantum di bawah ini. Anda mungkin menemukan informasi ini berguna ketika Anda memutuskan apakah akan menggunakan fitur caching kunci data, dan ketika Anda menetapkan ambang keamanan pada pengelola bahan kriptografi caching (caching CMM).

Entri Cache untuk Permintaan Enkripsi

Entri yang ditambahkan ke cache kunci data sebagai hasil dari operasi enkripsi mencakup elemen-elemen berikut:

- Kunci data teks biasa
- Kunci data terenkripsi (satu atau lebih)
- Konteks enkripsi
- Kunci penandatanganan pesan (jika digunakan)
- Suite algoritma
- Metadata, termasuk penghitung penggunaan untuk menegakkan ambang keamanan

Entri Cache untuk Permintaan Dekripsi

Entri yang ditambahkan ke cache kunci data sebagai hasil dari operasi dekripsi mencakup elemen-elemen berikut:

- Kunci data teks biasa
- Kunci verifikasi tanda tangan (jika digunakan)

- Metadata, termasuk penghitung penggunaan untuk menegakkan ambang keamanan

Konteks enkripsi: Cara memilih entri cache

Anda dapat menentukan konteks enkripsi dalam permintaan apa pun untuk mengenkripsi data. Namun, konteks enkripsi memainkan peran khusus dalam caching kunci data. Ini memungkinkan Anda membuat subkelompok kunci data di cache Anda, bahkan ketika kunci data berasal dari CMM caching yang sama.

Konteks enkripsi adalah seperangkat pasangan nilai kunci yang berisi data non-rahasia yang berubah-ubah. Selama enkripsi, konteks enkripsi terikat secara kriptografis ke data terenkripsi sehingga konteks enkripsi yang sama diperlukan untuk mendekripsi data. Dalam AWS Encryption SDK, konteks enkripsi disimpan dalam pesan terenkripsi dengan data terenkripsi dan kunci data.

Bila Anda menggunakan cache kunci data, Anda juga dapat menggunakan konteks enkripsi untuk memilih kunci data cache tertentu untuk operasi enkripsi Anda. Konteks enkripsi disimpan dalam entri cache dengan kunci data (ini adalah bagian dari ID entri cache). Kunci data yang di-cache hanya digunakan kembali jika konteks enkripsi mereka cocok. Jika Anda ingin menggunakan kembali kunci data tertentu untuk permintaan enkripsi, tentukan konteks enkripsi yang sama. Jika Anda ingin menghindari kunci data tersebut, tentukan konteks enkripsi yang berbeda.

Konteks enkripsi selalu opsional, tetapi disarankan. Jika Anda tidak menentukan konteks enkripsi dalam permintaan Anda, konteks enkripsi kosong disertakan dalam pengenal entri cache dan dicocokkan dengan setiap permintaan.

Apakah aplikasi saya menggunakan kunci data cache?

Data key caching adalah strategi optimasi yang sangat efektif untuk aplikasi dan beban kerja tertentu. Namun, karena mengandung beberapa risiko, penting untuk menentukan seberapa efektif kemungkinan untuk situasi Anda, dan kemudian memutuskan apakah manfaatnya lebih besar daripada risikonya.

Karena caching kunci data menggunakan kembali kunci data, efek yang paling jelas adalah mengurangi jumlah panggilan untuk menghasilkan kunci data baru. Ketika caching kunci data diimplementasikan, AWS Encryption SDK panggilan AWS KMS `GenerateDataKey` operasi hanya untuk membuat kunci data awal dan ketika cache meleset. Namun, caching meningkatkan kinerja secara nyata hanya dalam aplikasi yang menghasilkan banyak kunci data dengan karakteristik yang sama, termasuk konteks enkripsi dan rangkaian algoritma yang sama.

Untuk menentukan apakah implementasi Anda AWS Encryption SDK benar-benar menggunakan kunci data dari cache, coba teknik berikut.

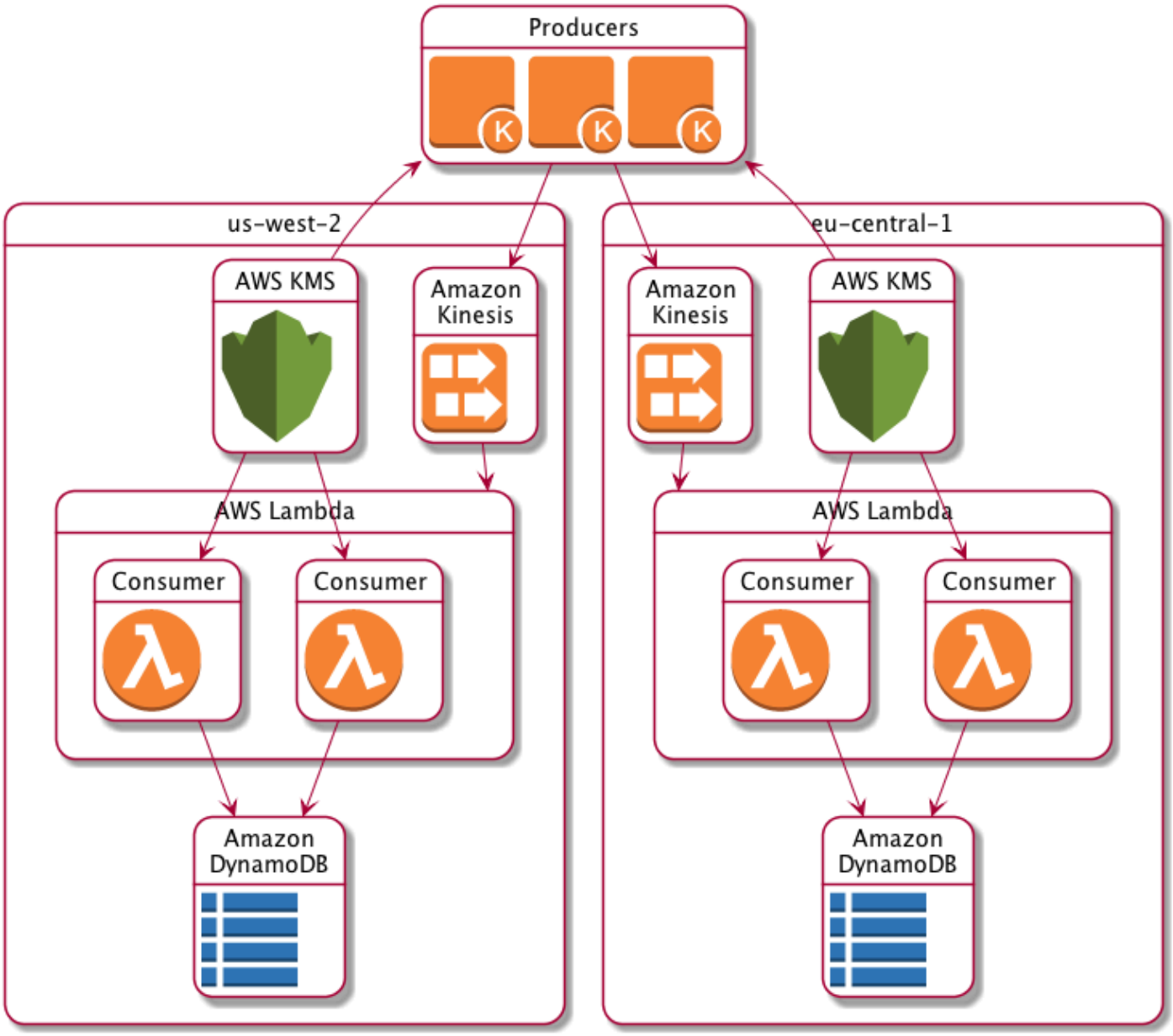
- Di log infrastruktur kunci master Anda, periksa frekuensi panggilan untuk membuat kunci data baru. Ketika caching kunci data efektif, jumlah panggilan untuk membuat kunci baru akan turun dengan jelas. Misalnya, jika Anda menggunakan penyedia kunci AWS KMS master atau keyring, cari CloudTrail log untuk GenerateDataKeypanggilan.
- Bandingkan pesan terenkripsi yang AWS Encryption SDK dikembalikan sebagai respons terhadap permintaan enkripsi yang berbeda. Misalnya, jika Anda menggunakan AWS Encryption SDK for Java, bandingkan ParsedCiphertextobjek dari panggilan enkripsi yang berbeda. Dalam AWS Encryption SDK for JavaScript, bandingkan isi `encryptedDataKeys` properti MessageHeader. Ketika kunci data digunakan kembali, kunci data terenkripsi dalam pesan terenkripsi identik.

Contoh caching kunci data

Contoh ini menggunakan caching kunci data dengan cache lokal untuk mempercepat aplikasi di mana data yang dihasilkan oleh beberapa perangkat dienkripsi dan disimpan di Wilayah yang berbeda.

Dalam skenario ini, beberapa produsen data menghasilkan data, mengenkripsi, dan menulis ke aliran Kinesis di setiap Wilayah. AWS Lambdafungsi (konsumen) mendekripsi aliran dan menulis data teks biasa ke tabel DynamoDB di Wilayah. Produsen data dan konsumen menggunakan AWS Encryption SDK dan penyedia kunci AWS KMS utama. Untuk mengurangi panggilan ke KMS, setiap produsen dan konsumen memiliki cache lokal mereka sendiri.

Anda dapat menemukan kode sumber untuk contoh-contoh ini di Java dan Python. Sampel juga menyertakan CloudFormation template yang mendefinisikan sumber daya untuk sampel.



Hasil cache lokal

Tabel berikut menunjukkan bahwa cache lokal mengurangi total panggilan ke KMS (per detik per Wilayah) dalam contoh ini menjadi 1% dari nilai aslinya.

Permintaan produsen

	Permintaan per detik per klien	Klien per wilayah	Permintaan rata-rata

	Hasilkan kunci data (us-west-2)	Enkripsi kunci data (eu-central-1)	Total (per wilayah)		per detik per wilayah
Tidak ada cache	1	1	1	500	500
Cache lokal	1 rps/100 penggunaan	1 rps/100 penggunaan	1 rps/100 penggunaan	500	5

Permintaan konsumen

	Permintaan per detik per klien			Klien per wilayah	Permintaan rata-rata per detik per wilayah
	Dekripsi kunci data	Produser	Total		
Tidak ada cache	1 rps per produsen	500	500	2	1.000
Cache lokal	1 rps per produsen/100 penggunaan	500	5	2	10

Kode contoh caching kunci data

Contoh kode ini menciptakan implementasi sederhana dari caching kunci data dengan cache lokal di Java dan Python. Kode ini menciptakan dua contoh cache lokal: satu untuk produsen data yang mengenkripsi data dan satu lagi untuk konsumen data (AWS Lambda fungsi) yang mendekripsi data. Untuk detail tentang implementasi caching kunci data dalam setiap bahasa, lihat dokumentasi Javadoc dan Python untuk. AWS Encryption SDK

Data key caching tersedia untuk semua bahasa pemrograman yang AWS Encryption SDK mendukung.

Untuk contoh lengkap dan teruji menggunakan caching kunci data di AWS Encryption SDK, lihat:

- C/C++: caching_cmm.cpp

- Jawa: SimpleDataKeyCachingExample.java
- JavaScript Peramban: caching_cmm.ts
- JavaScript Node.js: caching_cmm.ts
- Python: data_key_caching_basic.py

Produser

Produser mendapatkan peta, mengubahnya menjadi JSON, menggunakan AWS Encryption SDK untuk mengenkripsi, dan mendorong catatan ciphertext ke aliran Kinesis di masing-masing. Wilayah AWS

Kode mendefinisikan manajer bahan kriptografi caching (caching CMM) dan mengaitkannya dengan cache lokal dan penyedia kunci master yang mendasarinya.AWS KMS CMM caching menyimpan kunci data (dan materi kriptografi terkait) dari penyedia kunci utama. Ini juga berinteraksi dengan cache atas nama SDK dan memberlakukan ambang keamanan yang Anda tetapkan.

Karena panggilan ke metode enkripsi menentukan CMM caching, bukan manajer bahan kriptografi biasa (CMM) atau penyedia kunci utama, enkripsi akan menggunakan caching kunci data.

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x dari CMM AWS Encryption SDK for Java caching kunci data tidak digunakan lagi. Dengan versi 3. x, Anda juga dapat menggunakan keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

```
/*
 * Copyright 2017 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License"). You may not use
 this file except
 * in compliance with the License. A copy of the License is located at
 *
 * http://aws.amazon.com/apache2.0
 *
 * or in the "license" file accompanying this file. This file is distributed on an
 "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the
 License for the
 * specific language governing permissions and limitations under the License.
 */
```

```
package com.amazonaws.crypto.examples.kinesisdatakeycaching;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CommitmentPolicy;
import com.amazonaws.encryptionsdk.CryptoResult;
import com.amazonaws.encryptionsdk.MasterKeyProvider;
import com.amazonaws.encryptionsdk.caching.CachingCryptoMaterialsManager;
import com.amazonaws.encryptionsdk.caching.LocalCryptoMaterialsCache;
import com.amazonaws.encryptionsdk.kmssdkv2.KmsMasterKey;
import com.amazonaws.encryptionsdk.kmssdkv2.KmsMasterKeyProvider;
import com.amazonaws.encryptionsdk.multi.MultipleProviderFactory;
import com.amazonaws.util.json.Jackson;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import java.util.UUID;
import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.kinesis.KinesisClient;
import software.amazon.awssdk.services.kms.KmsClient;

/**
 * Pushes data to Kinesis Streams in multiple Regions.
 */
public class MultiRegionRecordPusher {

    private static final long MAX_ENTRY_AGE_MILLISECONDS = 300000;
    private static final long MAX_ENTRY_USES = 100;
    private static final int MAX_CACHE_ENTRIES = 100;
    private final String streamName_;
    private final ArrayList<KinesisClient> kinesisClients_;
    private final CachingCryptoMaterialsManager cachingMaterialsManager_;
    private final AwsCrypto crypto_;

    /**
     * Creates an instance of this object with Kinesis clients for all target
 Regions and a cached
     * key provider containing KMS master keys in all target Regions.
     */
```

```
   public MultiRegionRecordPusher(final Region[] regions, final String
kmsAliasName,
       final String streamName) {
       streamName_ = streamName;
       crypto_ = AwsCrypto.builder()
           .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
           .build();
       kinesisClients_ = new ArrayList<>();

       AwsCredentialsProvider credentialsProvider =
DefaultCredentialsProvider.builder().build();

       // Build KmsMasterKey and AmazonKinesisClient objects for each target region
       List<KmsMasterKey> masterKeys = new ArrayList<>();
       for (Region region : regions) {
           kinesisClients_.add(KinesisClient.builder()
               .credentialsProvider(credentialsProvider)
               .region(region)
               .build());

           KmsMasterKey regionMasterKey = KmsMasterKeyProvider.builder()
               .defaultRegion(region)
               .builderSupplier(() ->
KmsClient.builder().credentialsProvider(credentialsProvider))
               .buildStrict(kmsAliasName)
               .getMasterKey(kmsAliasName);

           masterKeys.add(regionMasterKey);
       }

       // Collect KmsMasterKey objects into single provider and add cache
       MasterKeyProvider<?> masterKeyProvider =
MultipleProviderFactory.buildMultiProvider(
           KmsMasterKey.class,
           masterKeys
       );

       cachingMaterialsManager_ = CachingCryptoMaterialsManager.newBuilder()
           .withMasterKeyProvider(masterKeyProvider)
           .withCache(new LocalCryptoMaterialsCache(MAX_CACHE_ENTRIES))
           .withMaxAge(MAX_ENTRY_AGE_MILLISECONDS, TimeUnit.MILLISECONDS)
           .withMessageUseLimit(MAX_ENTRY_USES)
           .build();
   }
```

```
    /**
     * JSON serializes and encrypts the received record data and pushes it to all
 target streams.
     */
    public void putRecord(final Map<Object, Object> data) {
        String partitionKey = UUID.randomUUID().toString();
        Map<String, String> encryptionContext = new HashMap<>();
        encryptionContext.put("stream", streamName_);

        // JSON serialize data
        String jsonData = Jackson.toJsonString(data);

        // Encrypt data
        CryptoResult<byte[], ?> result = crypto_.encryptData(
            cachingMaterialsManager_,
            jsonData.getBytes(),
            encryptionContext
        );
        byte[] encryptedData = result.getResult();

        // Put records to Kinesis stream in all Regions
        for (KinesisClient regionalKinesisClient : kinesisClients_) {
            regionalKinesisClient.putRecord(builder ->
                builder.streamName(streamName_)
                    .data(SdkBytes.fromByteArray(encryptedData))
                    .partitionKey(partitionKey));
        }
    }
}
```

Python

```
"""
Copyright 2017 Amazon.com, Inc. or its affiliates. All Rights Reserved.

Licensed under the Apache License, Version 2.0 (the "License"). You may not use this
 file except
in compliance with the License. A copy of the License is located at

https://aws.amazon.com/apache-2-0/
```

```
or in the "license" file accompanying this file. This file is distributed on an "AS
 IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the
 License for the
specific language governing permissions and limitations under the License.
"""
import json
import uuid

from aws_encryption_sdk import EncryptionSDKClient, StrictAwsKmsMasterKeyProvider,
 CachingCryptoMaterialsManager, LocalCryptoMaterialsCache, CommitmentPolicy
from aws_encryption_sdk.key_providers.kms import KMSMasterKey
import boto3


class MultiRegionRecordPusher(object):
    """Pushes data to Kinesis Streams in multiple Regions."""
    CACHE_CAPACITY = 100
    MAX_ENTRY_AGE_SECONDS = 300.0
    MAX_ENTRY_MESSAGES_ENCRYPTED = 100

    def __init__(self, regions, kms_alias_name, stream_name):
        self._kinesis_clients = []
        self._stream_name = stream_name

        # Set up EncryptionSDKClient
        _client =
 EncryptionSDKClient(CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT)

        # Set up KMSMasterKeyProvider with cache
        _key_provider = StrictAwsKmsMasterKeyProvider(kms_alias_name)

        # Add MasterKey and Kinesis client for each Region
        for region in regions:
            self._kinesis_clients.append(boto3.client('kinesis',
 region_name=region))
            regional_master_key = KMSMasterKey(
                client=boto3.client('kms', region_name=region),
                key_id=kms_alias_name
            )
            _key_provider.add_master_key_provider(regional_master_key)

        cache = LocalCryptoMaterialsCache(capacity=self.CACHE_CAPACITY)
        self._materials_manager = CachingCryptoMaterialsManager(
```

```
            master_key_provider=_key_provider,
            cache=cache,
            max_age=self.MAX_ENTRY_AGE_SECONDS,
            max_messages_encrypted=self.MAX_ENTRY_MESSAGES_ENCRYPTED
        )

    def put_record(self, record_data):
        """JSON serializes and encrypts the received record data and pushes it to
all target streams.

        :param dict record_data: Data to write to stream
        """
        # Kinesis partition key to randomize write load across stream shards
        partition_key = uuid.uuid4().hex

        encryption_context = {'stream': self._stream_name}

        # JSON serialize data
        json_data = json.dumps(record_data)

        # Encrypt data
        encrypted_data, _header = _client.encrypt(
            source=json_data,
            materials_manager=self._materials_manager,
            encryption_context=encryption_context
        )

        # Put records to Kinesis stream in all Regions
        for client in self._kinesis_clients:
            client.put_record(
                StreamName=self._stream_name,
                Data=encrypted_data,
                PartitionKey=partition_key
            )
```

Konsumen

Konsumen data adalah AWS Lambdafungsi yang dipicu oleh peristiwa Kinesis. Ini mendekripsi dan deserialisasi setiap catatan, dan menulis catatan teks biasa ke tabel Amazon DynamoDB di Wilayah yang sama.

Seperti kode produsen, kode konsumen memungkinkan caching kunci data dengan menggunakan manajer bahan kriptografi caching (caching CMM) dalam panggilan ke metode dekripsi.

Kode Java membangun penyedia kunci master dalam mode ketat dengan yang ditentukan AWS KMS key. Mode ketat tidak diperlukan saat mendekripsi, tetapi ini adalah praktik terbaik. Kode Python menggunakan mode penemuan, yang memungkinkan AWS Encryption SDK penggunaan kunci pembungkus apa pun yang mengenkripsi kunci data untuk mendekripsi itu.

Java

Contoh berikut menggunakan versi 2. x dari AWS Encryption SDK for Java. Versi 3. x dari CMM AWS Encryption SDK for Java caching kunci data tidak digunakan lagi. Dengan versi 3. x, Anda juga dapat menggunakan keyring AWS KMS Hierarkis, solusi caching bahan kriptografi alternatif.

Kode ini membuat penyedia kunci master untuk mendekripsi dalam mode ketat. Hanya AWS Encryption SDK dapat menggunakan yang AWS KMS keys Anda tentukan untuk mendekripsi pesan Anda.

```
/*
 * Copyright 2017 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * Licensed under the Apache License, Version 2.0 (the "License"). You may not use
 this file except
 * in compliance with the License. A copy of the License is located at
 *
 * http://aws.amazon.com/apache2.0
 *
 * or in the "license" file accompanying this file. This file is distributed on an
 "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the
 License for the
 * specific language governing permissions and limitations under the License.
 */
package com.amazonaws.crypto.examples.kinesisdatakeycaching;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CommitmentPolicy;
import com.amazonaws.encryptionsdk.CryptoResult;
import com.amazonaws.encryptionsdk.caching.CachingCryptoMaterialsManager;
import com.amazonaws.encryptionsdk.caching.LocalCryptoMaterialsCache;
import com.amazonaws.encryptionsdk.kmssdkv2.KmsMasterKeyProvider;
import com.amazonaws.services.lambda.runtime.Context;
```

```
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent.KinesisEventRecord;
import com.amazonaws.util.BinaryUtils;
import java.io.UnsupportedEncodingException;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.enhanced.dynamodb.DynamoDbEnhancedClient;
import software.amazon.awssdk.enhanced.dynamodb.DynamoDbTable;
import software.amazon.awssdk.enhanced.dynamodb.TableSchema;

/**
 * Decrypts all incoming Kinesis records and writes records to DynamoDB.
 */
public class LambdaDecryptAndWrite {

    private static final long MAX_ENTRY_AGE_MILLISECONDS = 600000;
    private static final int MAX_CACHE_ENTRIES = 100;
    private final CachingCryptoMaterialsManager cachingMaterialsManager_;
    private final AwsCrypto crypto_;
    private final DynamoDbTable<Item> table_;

    /**
     * Because the cache is used only for decryption, the code doesn't set the max
 bytes or max
     * message security thresholds that are enforced only on on data keys used for
 encryption.
     */
    public LambdaDecryptAndWrite() {
        String kmsKeyArn = System.getenv("CMK_ARN");
        cachingMaterialsManager_ = CachingCryptoMaterialsManager.newBuilder()

 .withMasterKeyProvider(KmsMasterKeyProvider.builder().buildStrict(kmsKeyArn))
            .withCache(new LocalCryptoMaterialsCache(MAX_CACHE_ENTRIES))
            .withMaxAge(MAX_ENTRY_AGE_MILLISECONDS, TimeUnit.MILLISECONDS)
            .build();

        crypto_ = AwsCrypto.builder()
            .withCommitmentPolicy(CommitmentPolicy.RequireEncryptRequireDecrypt)
            .build();

        String tableName = System.getenv("TABLE_NAME");
        DynamoDbEnhancedClient dynamodb = DynamoDbEnhancedClient.builder().build();
        table_ = dynamodb.table(tableName, TableSchema.fromClass(Item.class));
```

```
    }

    /**
     * @param event
     * @param context
     */
    public void handleRequest(KinesisEvent event, Context context)
        throws UnsupportedEncodingException {
        for (KinesisEventRecord record : event.getRecords()) {
            ByteBuffer ciphertextBuffer = record.getKinesis().getData();
            byte[] ciphertext = BinaryUtils.copyAllBytesFrom(ciphertextBuffer);

            // Decrypt and unpack record
            CryptoResult<byte[], ?> plaintextResult =
 crypto_.decryptData(cachingMaterialsManager_,
                ciphertext);

            // Verify the encryption context value
            String streamArn = record.getEventSourceARN();
            String streamName = streamArn.substring(streamArn.indexOf("/") + 1);
            if (!
streamName.equals(plaintextResult.getEncryptionContext().get("stream"))) {
                throw new IllegalStateException("Wrong Encryption Context!");
            }

            // Write record to DynamoDB
            String jsonItem = new String(plaintextResult.getResult(),
 StandardCharsets.UTF_8);
            System.out.println(jsonItem);
            table_.putItem(Item.fromJSON(jsonItem));
        }
    }

    private static class Item {

        static Item fromJSON(String jsonText) {
            // Parse JSON and create new Item
            return new Item();
        }
    }
}
```

Python

Kode Python ini mendekripsi dengan penyedia kunci master dalam mode penemuan. Ini memungkinkan AWS Encryption SDK penggunaan kunci pembungkus apa pun yang mengenkripsi kunci data untuk mendekripsi itu. Mode ketat, di mana Anda menentukan kunci pembungkus yang dapat digunakan untuk dekripsi, adalah praktik terbaik.

```
"""
Copyright 2017 Amazon.com, Inc. or its affiliates. All Rights Reserved.

Licensed under the Apache License, Version 2.0 (the "License"). You may not use this
 file except
in compliance with the License. A copy of the License is located at

https://aws.amazon.com/apache-2-0/

or in the "license" file accompanying this file. This file is distributed on an "AS
 IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the
 License for the
specific language governing permissions and limitations under the License.
"""
import base64
import json
import logging
import os

from aws_encryption_sdk import EncryptionSDKClient,
 DiscoveryAwsKmsMasterKeyProvider, CachingCryptoMaterialsManager,
 LocalCryptoMaterialsCache, CommitmentPolicy
import boto3

_LOGGER = logging.getLogger(__name__)
_is_setup = False
CACHE_CAPACITY = 100
MAX_ENTRY_AGE_SECONDS = 600.0

def setup():
    """Sets up clients that should persist across Lambda invocations."""
    global encryption_sdk_client
    encryption_sdk_client =
 EncryptionSDKClient(CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT)
```

```
    global materials_manager
    key_provider = DiscoveryAwsKmsMasterKeyProvider()
    cache = LocalCryptoMaterialsCache(capacity=CACHE_CAPACITY)

    #  Because the cache is used only for decryption, the code doesn't set
    #   the max bytes or max message security thresholds that are enforced
    #   only on on data keys used for encryption.
    materials_manager = CachingCryptoMaterialsManager(
        master_key_provider=key_provider,
        cache=cache,
        max_age=MAX_ENTRY_AGE_SECONDS
    )
    global table
    table_name = os.environ.get('TABLE_NAME')
    table = boto3.resource('dynamodb').Table(table_name)
    global _is_setup
    _is_setup = True


def lambda_handler(event, context):
    """Decrypts all incoming Kinesis records and writes records to DynamoDB."""
    _LOGGER.debug('New event:')
    _LOGGER.debug(event)
    if not _is_setup:
        setup()
    with table.batch_writer() as batch:
        for record in event.get('Records', []):
            # Record data base64-encoded by Kinesis
            ciphertext = base64.b64decode(record['kinesis']['data'])

            # Decrypt and unpack record
            plaintext, header = encryption_sdk_client.decrypt(
                source=ciphertext,
                materials_manager=materials_manager
            )
            item = json.loads(plaintext)

            # Verify the encryption context value
            stream_name = record['eventSourceARN'].split('/', 1)[1]
            if stream_name != header.encryption_context['stream']:
                raise ValueError('Wrong Encryption Context!')

            # Write record to DynamoDB
            batch.put_item(Item=item)
```

Contoh caching kunci data: template CloudFormation

CloudFormation Template ini mengatur semua AWS sumber daya yang diperlukan untuk mereproduksi contoh caching kunci data.

JSON

```
{
    "Parameters": {
        "SourceCodeBucket": {
            "Type": "String",
            "Description": "S3 bucket containing Lambda source code zip files"
        },
        "PythonLambdaS3Key": {
            "Type": "String",
            "Description": "S3 key containing Python Lambda source code zip file"
        },
        "PythonLambdaObjectVersionId": {
            "Type": "String",
            "Description": "S3 version id for S3 key containing Python Lambda source
 code zip file"
        },
        "JavaLambdaS3Key": {
            "Type": "String",
            "Description": "S3 key containing Python Lambda source code zip file"
        },
        "JavaLambdaObjectVersionId": {
            "Type": "String",
            "Description": "S3 version id for S3 key containing Python Lambda source
 code zip file"
        },
        "KeyAliasSuffix": {
            "Type": "String",
            "Description": "Suffix to use for KMS key Alias (ie: alias/
KeyAliasSuffix)"
        },
        "StreamName": {
            "Type": "String",
            "Description": "Name to use for Kinesis Stream"
        }
```

```
    },
    "Resources": {
        "InputStream": {
            "Type": "AWS::Kinesis::Stream",
            "Properties": {
                "Name": {
                    "Ref": "StreamName"
                },
                "ShardCount": 2
            }
        },
        "PythonLambdaOutputTable": {
            "Type": "AWS::DynamoDB::Table",
            "Properties": {
                "AttributeDefinitions": [
                    {
                        "AttributeName": "id",
                        "AttributeType": "S"
                    }
                ],
                "KeySchema": [
                    {
                        "AttributeName": "id",
                        "KeyType": "HASH"
                    }
                ],
                "ProvisionedThroughput": {
                    "ReadCapacityUnits": 1,
                    "WriteCapacityUnits": 1
                }
            }
        },
        "PythonLambdaRole": {
            "Type": "AWS::IAM::Role",
            "Properties": {
                "AssumeRolePolicyDocument": {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Principal": {
                                "Service": "lambda.amazonaws.com"
                            },
                            "Action": "sts:AssumeRole"
```

```
                        }
                    ]
                },
                "ManagedPolicyArns": [
                    "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"
                ],
                "Policies": [
                    {
                        "PolicyName": "PythonLambdaAccess",
                        "PolicyDocument": {
                            "Version": "2012-10-17",
                            "Statement": [
                                {
                                    "Effect": "Allow",
                                    "Action": [
                                        "dynamodb:DescribeTable",
                                        "dynamodb:BatchWriteItem"
                                    ],
                                    "Resource": {
                                        "Fn::Sub": "arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${PythonLambdaOutputTable}"
                                    }
                                },
                                {
                                    "Effect": "Allow",
                                    "Action": [
                                        "dynamodb:PutItem"
                                    ],
                                    "Resource": {
                                        "Fn::Sub": "arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${PythonLambdaOutputTable}*"
                                    }
                                },
                                {
                                    "Effect": "Allow",
                                    "Action": [
                                        "kinesis:GetRecords",
                                        "kinesis:GetShardIterator",
                                        "kinesis:DescribeStream",
                                        "kinesis:ListStreams"
                                    ],
                                    "Resource": {
```

```
                                        "Fn::Sub": "arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}"
                                    }
                                }
                            ]
                        }
                    }
                ]
            }
        },
        "PythonLambdaFunction": {
            "Type": "AWS::Lambda::Function",
            "Properties": {
                "Description": "Python consumer",
                "Runtime": "python2.7",
                "MemorySize": 512,
                "Timeout": 90,
                "Role": {
                    "Fn::GetAtt": [
                        "PythonLambdaRole",
                        "Arn"
                    ]
                },
                "Handler":
 "aws_crypto_examples.kinesis_datakey_caching.consumer.lambda_handler",
                "Code": {
                    "S3Bucket": {
                        "Ref": "SourceCodeBucket"
                    },
                    "S3Key": {
                        "Ref": "PythonLambdaS3Key"
                    },
                    "S3ObjectVersion": {
                        "Ref": "PythonLambdaObjectVersionId"
                    }
                },
                "Environment": {
                    "Variables": {
                        "TABLE_NAME": {
                            "Ref": "PythonLambdaOutputTable"
                        }
                    }
                }
            }
```

```
        },
        "PythonLambdaSourceMapping": {
            "Type": "AWS::Lambda::EventSourceMapping",
            "Properties": {
                "BatchSize": 1,
                "Enabled": true,
                "EventSourceArn": {
                    "Fn::Sub": "arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}"
                },
                "FunctionName": {
                    "Ref": "PythonLambdaFunction"
                },
                "StartingPosition": "TRIM_HORIZON"
            }
        },
        "JavaLambdaOutputTable": {
            "Type": "AWS::DynamoDB::Table",
            "Properties": {
                "AttributeDefinitions": [
                    {
                        "AttributeName": "id",
                        "AttributeType": "S"
                    }
                ],
                "KeySchema": [
                    {
                        "AttributeName": "id",
                        "KeyType": "HASH"
                    }
                ],
                "ProvisionedThroughput": {
                    "ReadCapacityUnits": 1,
                    "WriteCapacityUnits": 1
                }
            }
        },
        "JavaLambdaRole": {
            "Type": "AWS::IAM::Role",
            "Properties": {
                "AssumeRolePolicyDocument": {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
```

```
                            "Effect": "Allow",
                            "Principal": {
                                "Service": "lambda.amazonaws.com"
                            },
                            "Action": "sts:AssumeRole"
                        }
                    ]
                },
                "ManagedPolicyArns": [
                    "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"
                ],
                "Policies": [
                    {
                        "PolicyName": "JavaLambdaAccess",
                        "PolicyDocument": {
                            "Version": "2012-10-17",
                            "Statement": [
                                {
                                    "Effect": "Allow",
                                    "Action": [
                                        "dynamodb:DescribeTable",
                                        "dynamodb:BatchWriteItem"
                                    ],
                                    "Resource": {
                                        "Fn::Sub": "arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${JavaLambdaOutputTable}"
                                    }
                                },
                                {
                                    "Effect": "Allow",
                                    "Action": [
                                        "dynamodb:PutItem"
                                    ],
                                    "Resource": {
                                        "Fn::Sub": "arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${JavaLambdaOutputTable}*"
                                    }
                                },
                                {
                                    "Effect": "Allow",
                                    "Action": [
                                        "kinesis:GetRecords",
                                        "kinesis:GetShardIterator",
```

```
                                        "kinesis:DescribeStream",
                                        "kinesis:ListStreams"
                                    ],
                                    "Resource": {
                                        "Fn::Sub": "arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}"
                                    }
                                }
                            ]
                        }
                    }
                ]
            }
        },
        "JavaLambdaFunction": {
            "Type": "AWS::Lambda::Function",
            "Properties": {
                "Description": "Java consumer",
                "Runtime": "java8",
                "MemorySize": 512,
                "Timeout": 90,
                "Role": {
                    "Fn::GetAtt": [
                        "JavaLambdaRole",
                        "Arn"
                    ]
                },
                "Handler":
 "com.amazonaws.crypto.examples.kinesisdatakeycaching.LambdaDecryptAndWrite::handleRequest",
                "Code": {
                    "S3Bucket": {
                        "Ref": "SourceCodeBucket"
                    },
                    "S3Key": {
                        "Ref": "JavaLambdaS3Key"
                    },
                    "S3ObjectVersion": {
                        "Ref": "JavaLambdaObjectVersionId"
                    }
                },
                "Environment": {
                    "Variables": {
                        "TABLE_NAME": {
                            "Ref": "JavaLambdaOutputTable"
```

```
                        },
                        "CMK_ARN": {
                            "Fn::GetAtt": [
                                "RegionKinesisCMK",
                                "Arn"
                            ]
                        }
                    }
                }
            }
        },
        "JavaLambdaSourceMapping": {
            "Type": "AWS::Lambda::EventSourceMapping",
            "Properties": {
                "BatchSize": 1,
                "Enabled": true,
                "EventSourceArn": {
                    "Fn::Sub": "arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}"
                },
                "FunctionName": {
                    "Ref": "JavaLambdaFunction"
                },
                "StartingPosition": "TRIM_HORIZON"
            }
        },
        "RegionKinesisCMK": {
            "Type": "AWS::KMS::Key",
            "Properties": {
                "Description": "Used to encrypt data passing through Kinesis Stream
 in this region",
                "Enabled": true,
                "KeyPolicy": {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Principal": {
                                "AWS": {
                                    "Fn::Sub": "arn:aws:iam::${AWS::AccountId}:root"
                                }
                            },
                            "Action": [
                                "kms:Encrypt",
```

```
                            "kms:GenerateDataKey",
                            "kms:CreateAlias",
                            "kms:DeleteAlias",
                            "kms:DescribeKey",
                            "kms:DisableKey",
                            "kms:EnableKey",
                            "kms:PutKeyPolicy",
                            "kms:ScheduleKeyDeletion",
                            "kms:UpdateAlias",
                            "kms:UpdateKeyDescription"
                        ],
                        "Resource": "*"
                    },
                    {
                        "Effect": "Allow",
                        "Principal": {
                            "AWS": [
                                {
                                    "Fn::GetAtt": [
                                        "PythonLambdaRole",
                                        "Arn"
                                    ]
                                },
                                {
                                    "Fn::GetAtt": [
                                        "JavaLambdaRole",
                                        "Arn"
                                    ]
                                }
                            ]
                        },
                        "Action": "kms:Decrypt",
                        "Resource": "*"
                    }
                ]
            }
        }
    },
    "RegionKinesisCMKAlias": {
        "Type": "AWS::KMS::Alias",
        "Properties": {
            "AliasName": {
                "Fn::Sub": "alias/${KeyAliasSuffix}"
            },
```

```
                "TargetKeyId": {
                    "Ref": "RegionKinesisCMK"
                }
            }
        }
    }
}
```

YAML

```
Parameters:
    SourceCodeBucket:
        Type: String
        Description: S3 bucket containing Lambda source code zip files
    PythonLambdaS3Key:
        Type: String
        Description: S3 key containing Python Lambda source code zip file
    PythonLambdaObjectVersionId:
        Type: String
        Description: S3 version id for S3 key containing Python Lambda source code
 zip file
    JavaLambdaS3Key:
        Type: String
        Description: S3 key containing Python Lambda source code zip file
    JavaLambdaObjectVersionId:
        Type: String
        Description: S3 version id for S3 key containing Python Lambda source code
 zip file
    KeyAliasSuffix:
        Type: String
        Description: 'Suffix to use for KMS CMK Alias (ie: alias/<KeyAliasSuffix>)'
    StreamName:
        Type: String
        Description: Name to use for Kinesis Stream
Resources:
    InputStream:
        Type: AWS::Kinesis::Stream
        Properties:
            Name: !Ref StreamName
            ShardCount: 2
    PythonLambdaOutputTable:
        Type: AWS::DynamoDB::Table
        Properties:
```

```
            AttributeDefinitions:
                -
                    AttributeName: id
                    AttributeType: S
            KeySchema:
                -
                    AttributeName: id
                    KeyType: HASH
            ProvisionedThroughput:
                ReadCapacityUnits: 1
                WriteCapacityUnits: 1
    PythonLambdaRole:
        Type: AWS::IAM::Role
        Properties:
            AssumeRolePolicyDocument:
                Version: 2012-10-17
                Statement:
                    -
                        Effect: Allow
                        Principal:
                            Service: lambda.amazonaws.com
                        Action: sts:AssumeRole
            ManagedPolicyArns:
                - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
            Policies:
                -
                    PolicyName: PythonLambdaAccess
                    PolicyDocument:
                        Version: 2012-10-17
                        Statement:
                            -
                                Effect: Allow
                                Action:
                                    - dynamodb:DescribeTable
                                    - dynamodb:BatchWriteItem
                                Resource: !Sub arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${PythonLambdaOutputTable}
                            -
                                Effect: Allow
                                Action:
                                    - dynamodb:PutItem
                                Resource: !Sub arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${PythonLambdaOutputTable}*
                            -
```

```
                                Effect: Allow
                                Action:
                                    - kinesis:GetRecords
                                    - kinesis:GetShardIterator
                                    - kinesis:DescribeStream
                                    - kinesis:ListStreams
                                Resource: !Sub arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}
    PythonLambdaFunction:
        Type: AWS::Lambda::Function
        Properties:
            Description: Python consumer
            Runtime: python2.7
            MemorySize: 512
            Timeout: 90
            Role: !GetAtt PythonLambdaRole.Arn
            Handler:
 aws_crypto_examples.kinesis_datakey_caching.consumer.lambda_handler
            Code:
                S3Bucket: !Ref SourceCodeBucket
                S3Key: !Ref PythonLambdaS3Key
                S3ObjectVersion: !Ref PythonLambdaObjectVersionId
            Environment:
                Variables:
                    TABLE_NAME: !Ref PythonLambdaOutputTable
    PythonLambdaSourceMapping:
        Type: AWS::Lambda::EventSourceMapping
        Properties:
            BatchSize: 1
            Enabled: true
            EventSourceArn: !Sub arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}
            FunctionName: !Ref PythonLambdaFunction
            StartingPosition: TRIM_HORIZON
    JavaLambdaOutputTable:
        Type: AWS::DynamoDB::Table
        Properties:
            AttributeDefinitions:
                -
                    AttributeName: id
                    AttributeType: S
            KeySchema:
                -
                    AttributeName: id
```

```
                    KeyType: HASH
            ProvisionedThroughput:
                ReadCapacityUnits: 1
                WriteCapacityUnits: 1
    JavaLambdaRole:
        Type: AWS::IAM::Role
        Properties:
            AssumeRolePolicyDocument:
                Version: 2012-10-17
                Statement:
                    -
                        Effect: Allow
                        Principal:
                            Service: lambda.amazonaws.com
                        Action: sts:AssumeRole
            ManagedPolicyArns:
                - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
            Policies:
                -
                    PolicyName: JavaLambdaAccess
                    PolicyDocument:
                        Version: 2012-10-17
                        Statement:
                            -
                                Effect: Allow
                                Action:
                                    - dynamodb:DescribeTable
                                    - dynamodb:BatchWriteItem
                                Resource: !Sub arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${JavaLambdaOutputTable}
                            -
                                Effect: Allow
                                Action:
                                    - dynamodb:PutItem
                                Resource: !Sub arn:aws:dynamodb:${AWS::Region}:
${AWS::AccountId}:table/${JavaLambdaOutputTable}*
                            -
                                Effect: Allow
                                Action:
                                    - kinesis:GetRecords
                                    - kinesis:GetShardIterator
                                    - kinesis:DescribeStream
                                    - kinesis:ListStreams
```

```
                                    Resource: !Sub arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}
    JavaLambdaFunction:
        Type: AWS::Lambda::Function
        Properties:
            Description: Java consumer
            Runtime: java8
            MemorySize: 512
            Timeout: 90
            Role: !GetAtt JavaLambdaRole.Arn
            Handler:
 com.amazonaws.crypto.examples.kinesisdatakeycaching.LambdaDecryptAndWrite::handleRequest
            Code:
                S3Bucket: !Ref SourceCodeBucket
                S3Key: !Ref JavaLambdaS3Key
                S3ObjectVersion: !Ref JavaLambdaObjectVersionId
            Environment:
                Variables:
                    TABLE_NAME: !Ref JavaLambdaOutputTable
                    CMK_ARN: !GetAtt RegionKinesisCMK.Arn
    JavaLambdaSourceMapping:
        Type: AWS::Lambda::EventSourceMapping
        Properties:
            BatchSize: 1
            Enabled: true
            EventSourceArn: !Sub arn:aws:kinesis:${AWS::Region}:
${AWS::AccountId}:stream/${InputStream}
            FunctionName: !Ref JavaLambdaFunction
            StartingPosition: TRIM_HORIZON
    RegionKinesisCMK:
        Type: AWS::KMS::Key
        Properties:
            Description: Used to encrypt data passing through Kinesis Stream in this
 region
            Enabled: true
            KeyPolicy:
                Version: 2012-10-17
                Statement:
                    -
                        Effect: Allow
                        Principal:
                            AWS: !Sub arn:aws:iam::${AWS::AccountId}:root
                        Action:
                            # Data plane actions
```

```
                            - kms:Encrypt
                            - kms:GenerateDataKey
                            # Control plane actions
                            - kms:CreateAlias
                            - kms:DeleteAlias
                            - kms:DescribeKey
                            - kms:DisableKey
                            - kms:EnableKey
                            - kms:PutKeyPolicy
                            - kms:ScheduleKeyDeletion
                            - kms:UpdateAlias
                            - kms:UpdateKeyDescription
                        Resource: '*'
                    -
                        Effect: Allow
                        Principal:
                            AWS:
                                - !GetAtt PythonLambdaRole.Arn
                                - !GetAtt JavaLambdaRole.Arn
                        Action: kms:Decrypt
                        Resource: '*'
    RegionKinesisCMKAlias:
        Type: AWS::KMS::Alias
        Properties:
            AliasName: !Sub alias/${KeyAliasSuffix}
            TargetKeyId: !Ref RegionKinesisCMK
```

Versi dari AWS Encryption SDK

Implementasi AWS Encryption SDK bahasa menggunakan versi semantik untuk memudahkan Anda mengidentifikasi besarnya perubahan di setiap rilis. Perubahan nomor versi utama, seperti 1. x. x ke 2. x. x, menunjukkan perubahan yang melanggar yang kemungkinan memerlukan perubahan kode dan penerapan yang direncanakan. Memecahkan perubahan dalam versi baru mungkin tidak memengaruhi setiap kasus penggunaan, tinjau catatan rilis untuk melihat apakah Anda terpengaruh. Perubahan dalam versi minor, seperti x .1. x ke x .2. x, selalu kompatibel ke belakang, tetapi mungkin menyertakan elemen usang.

Bila memungkinkan, gunakan versi terbaru dari AWS Encryption SDK dalam bahasa pemrograman pilihan Anda. Kebijakan pemeliharaan dan dukungan untuk setiap versi berbeda antara implementasi bahasa pemrograman. Untuk detail tentang versi yang didukung dalam bahasa pemrograman pilihan Anda, lihat `SUPPORT_POLICY.rst` file di GitHubrepositorinya.

Ketika peningkatan menyertakan fitur baru yang memerlukan konfigurasi khusus untuk menghindari kesalahan enkripsi atau dekripsi, kami menyediakan versi perantara dan instruksi terperinci untuk menggunakannya. Misalnya, versi 1.7. x dan 1.8. x dirancang untuk menjadi versi transisi yang membantu Anda meningkatkan dari versi lebih awal dari 1.7. x ke versi 2.0. x dan kemudian. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

> **Note**
>
> X dalam nomor versi mewakili patch dari versi mayor dan minor. Misalnya, versi 1.7. x mewakili semua versi yang dimulai dengan 1.7, termasuk 1.7.1 dan 1.7.9.
> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Tabel berikut memberikan gambaran tentang perbedaan utama antara versi yang didukung AWS Encryption SDK untuk setiap bahasa pemrograman.

C

Untuk penjelasan rinci tentang semua perubahan, lihat changeLog.md di repositori pada. aws-encryption-sdk-c GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
1.x	1.0	Rilis awal.	End-of-Support fase
	1.7	Pembaruan untuk AWS Encryption SDK yang membantu pengguna versi sebelumnya meningkatkan ke versi 2.0. x dan kemudian. Untuk informasi selengkapnya, lihat versi 1.7. x.	
2.x	2.0	Pembaruan untuk AWS Encryption SDK. Untuk informasi selengkapnya, lihat versi 2.0. x.	Ketersediaan Umum (GA)
	2.2	Perbaikan proses dekripsi pesan.	
	2.3	Menambahkan dukungan untuk kunci AWS KMS Multi-wil ayah.	

C #/.NET

Untuk penjelasan rinci tentang semua perubahan, lihat changeLog.md di repositori pada. `aws-encryption-sdk-net` GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
3.x	3.1.0	Pelepasan awal.	Akhir dukungan Versi 3.x AWS Encryption SDK untuk .NET telah memasuki End of Support; tolong, tingkatkan ke 4.x.
4.x	4.0	Menambahkan dukungan untuk keyring AWS KMS Hierarkis, CMM konteks enkripsi yang diperlukan, dan gantungan kunci RSA asimetris. AWS KMS	Ketersediaan Umum (GA)

Antarmuka baris perintah (CLI)

Untuk penjelasan rinci tentang semua perubahan, lihat Versi CLI AWS Enkripsi dan ChangeLog.rst di repositori pada. aws-encryption-sdk-cli GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
1.x	1.0	Rilis awal.	End-of-Support fase
	1.7	Pembaruan untuk AWS Encryption SDK yang membantu pengguna versi sebelumnya meningkatkan ke versi	

		2.0. x dan kemudian. Untuk informasi selengkapnya, lihat versi 1.7. x.	
2.x	2.0	Pembaruan untuk AWS Encryption SDK. Untuk informasi selengkapnya, lihat versi 2.0. x.	End-of-Support fase
	2.1	Menghapus `--discovery` parameter dan menggantinya dengan `discovery` atribut `--wrapping-keys` parameter. Versi 2.1.0 dari AWS Encryption CLI setara dengan versi 2.0 dalam bahasa pemrograman lainnya.	
	2.2	Perbaikan proses dekripsi pesan.	
3.x	3.0	Menambahkan dukungan untuk kunci AWS KMS Multi-wil ayah.	End-of-Support fase

4.x	4.0	AWS Enkripsi CLI tidak lagi mendukung Python 2 atau Python 3.4. Pada versi utama 4. x dari CLI AWS Enkripsi, hanya Python 3.5 atau yang lebih baru yang didukung.	Ketersediaan Umum (GA)
	4.1	AWS Enkripsi CLI tidak lagi mendukung Python 3.5. Pada versi 4.1. x dari CLI AWS Enkripsi, hanya Python 3.6 atau yang lebih baru yang didukung.	
	4.2	AWS Enkripsi CLI tidak lagi mendukung Python 3.6. Pada versi 4.2. x dari CLI AWS Enkripsi, hanya Python 3.7 atau yang lebih baru yang didukung.	

Java

Untuk penjelasan rinci tentang semua perubahan, lihat ChangeLog.rst di repositori pada. aws-encryption-sdk-java GitHub

Versi utama	Detail	Fase siklus hidup versi utama SDK

1.x	1.0	Rilis awal.	End-of-Support fase
	1.3	Menambahkan dukungan untuk pengelola materi kriptografi dan caching kunci data. Pindah ke generasi IV deterministik.	
	1.6.1	Mencela `AwsCrypto.encryptString()` dan menggantikannya dengan `AwsCrypto.decryptString()` dan. `AwsCrypto.encryptData()` `AwsCrypto.decryptData()`	
	1.7	Pembaruan untuk AWS Encryption SDK yang membantu pengguna versi sebelumnya meningkatkan ke versi 2.0. x dan kemudian. Untuk informasi selengkapnya, lihat versi 1.7. x.	

2.x	2.0	Pembaruan untuk AWS Encryption SDK. Untuk informasi selengkapnya, lihat versi 2.0. x.	Ketersediaan Umum (GA) Versi 2.x AWS Encryption SDK for Java akan memasuki mode pemeliharaan pada tahun 2024.
	2.2	Perbaikan proses dekripsi pesan.	
	2.3	Menambahkan dukungan untuk kunci AWS KMS Multi-wil ayah.	
	2.4	Menambahkan dukungan untuk AWS SDK for Java 2.x.	

3.x	3.0	Mengintegrasikan AWS Encryption SDK for Java dengan Material Providers Library (MPL). Menambahkan dukungan untuk gantungan kunci RSA simetris dan asimetris, AWS KMS gantungan kunci AWS KMS ECDH, gantungan kunci AWS KMS hierarkis, gantungan kunci Raw AES, gantungan kunci Raw RSA, gantungan kunci ECDH mentah, Multi-keyrings, dan konteks enkripsi CMM yang diperlukan.	Ketersediaan Umum (GA)

Go

Untuk penjelasan rinci tentang semua perubahan, lihat ChangeLog.md di direktori Go dari repositori pada. aws-encryption-sdk GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
0,1. x	0.1.0	Pelepasan awal.	Ketersediaan Umum (GA)

JavaScript

Untuk penjelasan rinci tentang semua perubahan, lihat changeLog.md di repositori pada. aws-encryption-sdk-javascript GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
1.x	1.0	Rilis awal.	End-of-Support fase
	1.7	Pembaruan untuk AWS Encryption SDK yang membantu pengguna versi sebelumnya meningkatkan ke versi 2.0. x dan kemudian. Untuk informasi selengkapnya, lihat versi 1.7. x.	
2.x	2.0	Pembaruan untuk AWS Encryption SDK. Untuk informasi selengkapnya, lihat versi 2.0. x.	End-of-Support fase
	2.2	Perbaikan proses dekripsi pesan.	
	2.3	Menambahkan dukungan untuk kunci AWS KMS Multi-wil ayah.	
3.x	3.0	Menghapus cakupan CI untuk Node 10. Upgrade dependens	Maintenance Support untuk versi 3.x AWS Encryption

		i agar tidak lagi mendukung Node 8 dan Node 10.	SDK for JavaScript akan berakhir pada 17 Januari 2024.
4.x	4.0	Memerlukan versi 3 dari AWS Encryption SDK for JavaScript's `kms-client` untuk menggunakan AWS KMS keyring.	Ketersediaan Umum (GA)

Python

Untuk penjelasan rinci tentang semua perubahan, lihat ChangeLog.rst di repositori pada. aws-encryption-sdk-python GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
1.x	1.0	Rilis awal.	End-of-Support fase
	1.3	Menambahkan dukungan untuk pengelola materi kriptografi dan caching kunci data. Pindah ke generasi IV deterministik.	
	1.7	Pembaruan untuk AWS Encryption SDK yang membantu pengguna versi sebelumnya meningkatkan ke versi 2.0. x dan kemudian. Untuk informasi	

		selengkapnya, lihat versi 1.7. x.	
2.x	2.0	Pembaruan untuk AWS Encryption SDK. Untuk informasi selengkapnya, lihat versi 2.0. x.	End-of-Support fase
	2.2	Perbaikan proses dekripsi pesan.	
	2.3	Menambahkan dukungan untuk kunci AWS KMS Multi-wil ayah.	
3.x	3.0	AWS Encryption SDK for Python Tidak lagi mendukung Python 2 atau Python 3.4. Pada versi utama 3. x dari AWS Encryptio n SDK for Python, hanya Python 3.5 atau yang lebih baru yang didukung.	Ketersediaan Umum (GA)
4.x	4.0	Mengintegrasikan AWS Encryption SDK for Python dengan Material Providers Library (MPL).	Ketersediaan Umum (GA)

Karat

Untuk penjelasan rinci tentang semua perubahan, lihat ChangeLog.md di direktori Rust dari repositori pada. aws-encryption-sdk GitHub

Versi utama	Detail		Fase siklus hidup versi utama SDK
1.x	1.0	Rilis awal.	Ketersediaan Umum (GA)

Detail versi

Daftar berikut menjelaskan perbedaan utama antara versi yang didukung dari AWS Encryption SDK.

Topik

Versi lebih awal dari 1.7. x

> **Note**
>
> Semua 1. x. x versi AWS Encryption SDK sedang dalam end-of-supportfase. Tingkatkan ke versi terbaru yang tersedia AWS Encryption SDK untuk bahasa pemrograman Anda sesegera mungkin. Untuk meng-upgrade dari AWS Encryption SDK versi lebih awal dari 1.7. x, Anda harus terlebih dahulu meng-upgrade ke 1.7. x. Lihat perinciannya di Migrasi Anda AWS Encryption SDK.

Versi yang AWS Encryption SDK lebih awal dari 1.7. x menyediakan fitur keamanan penting, termasuk enkripsi dengan algoritma Advanced Encryption Standard in Galois/Counter Mode (AES-

GCM), fungsi derivasi extract-and-expand kunci berbasis HMAC (HKDF), penandatanganan, dan kunci enkripsi 256-bit. Namun, versi ini tidak mendukung praktik terbaik yang kami rekomendasikan, termasuk komitmen utama.

Versi 1.7. x

> **Note**
>
> Semua 1. x. x versi AWS Encryption SDK sedang dalam end-of-supportfase.

Versi 1.7. x dirancang untuk membantu pengguna versi sebelumnya AWS Encryption SDK untuk meningkatkan ke versi 2.0. x dan kemudian. Jika Anda baru mengenal AWS Encryption SDK, Anda dapat melewati versi ini dan mulai dengan versi terbaru yang tersedia dalam bahasa pemrograman Anda.

Versi 1.7. x sepenuhnya kompatibel ke belakang; itu tidak memperkenalkan perubahan yang melanggar atau mengubah perilaku. AWS Encryption SDK Ini juga kompatibel ke depan; ini memungkinkan Anda untuk memperbarui kode Anda sehingga kompatibel dengan versi 2.0. x. Ini termasuk fitur baru, tetapi tidak sepenuhnya mengaktifkannya. Dan itu membutuhkan nilai konfigurasi yang mencegah Anda segera mengadopsi semua fitur baru sampai Anda siap.

Versi 1.7. x mencakup perubahan berikut:

AWS KMS pembaruan penyedia kunci master (wajib)

Versi 1.7. x memperkenalkan konstruktor baru ke AWS Encryption SDK for Java dan AWS Encryption SDK for Python yang secara eksplisit membuat penyedia kunci AWS KMS master baik dalam mode ketat atau penemuan. Versi ini menambahkan perubahan serupa pada antarmuka AWS Encryption SDK baris perintah (CLI). Lihat perinciannya di Memperbarui penyedia kunci AWS KMS utama.

- Dalam mode ketat, penyedia kunci AWS KMS master memerlukan daftar kunci pembungkus, dan mereka mengenkripsi dan mendekripsi hanya dengan kunci pembungkus yang Anda tentukan. Ini adalah praktik AWS Encryption SDK terbaik yang memastikan bahwa Anda menggunakan kunci pembungkus yang ingin Anda gunakan.
- Dalam mode penemuan, penyedia kunci AWS KMS master tidak mengambil kunci pembungkus apa pun. Anda tidak dapat menggunakannya untuk mengenkripsi. Saat mendekripsi, mereka dapat menggunakan kunci pembungkus apa pun untuk mendekripsi kunci data terenkripsi.

Namun, Anda dapat membatasi kunci pembungkus yang digunakan untuk dekripsi pada yang khusus. Akun AWS Pemfilteran akun bersifat opsional, tetapi ini adalah praktik terbaik yang kami rekomendasikan.

Konstruktor yang membuat versi sebelumnya dari penyedia kunci AWS KMS master tidak digunakan lagi di versi 1.7. x dan dihapus dalam versi 2.0. x. Konstruktor ini membuat instance penyedia kunci master yang mengenkripsi menggunakan kunci pembungkus yang Anda tentukan. Namun, mereka mendekripsi kunci data terenkripsi menggunakan kunci pembungkus yang mengenkripsi mereka, tanpa memperhatikan kunci pembungkus yang ditentukan. Pengguna mungkin secara tidak sengaja mendekripsi pesan dengan kunci pembungkus yang tidak ingin mereka gunakan, termasuk AWS KMS keys di lain dan Wilayah. Akun AWS

Tidak ada perubahan pada konstruktor untuk kunci AWS KMS master. Saat mengenkripsi dan mendekripsi, kunci AWS KMS master hanya menggunakan yang Anda tentukan. AWS KMS key

AWS KMS pembaruan keyring (opsional)

Versi 1.7. x menambahkan filter baru ke AWS Encryption SDK for C dan AWS Encryption SDK for JavaScript implementasi yang membatasi keyring AWS KMS penemuan ke tertentu. Akun AWS Filter akun baru ini bersifat opsional, tetapi ini adalah praktik terbaik yang kami rekomendasikan. Lihat perinciannya di Memperbarui AWS KMS keyrings.

Tidak ada perubahan pada konstruktor untuk AWS KMS gantungan kunci. AWS KMS Gantungan kunci standar berperilaku seperti penyedia kunci utama dalam mode ketat. AWS KMS keyrings penemuan dibuat secara eksplisit dalam mode penemuan.

Melewati ID kunci untuk AWS KMS Dekripsi

Dimulai pada versi 1.7. x, saat mendekripsi kunci data terenkripsi, AWS Encryption SDK selalu menentukan AWS KMS key dalam panggilannya ke operasi Dekripsi. AWS KMS AWS Encryption SDK Mendapatkan nilai ID kunci untuk AWS KMS key dari metadata di setiap kunci data terenkripsi. Fitur ini tidak memerlukan perubahan kode apa pun.

Menentukan ID kunci tidak AWS KMS key diperlukan untuk mendekripsi ciphertext yang dienkripsi di bawah kunci KMS enkripsi simetris, tetapi ini adalah praktik terbaik.AWS KMS Seperti menentukan kunci pembungkus di penyedia kunci Anda, praktik ini memastikan bahwa AWS KMS hanya mendekripsi menggunakan kunci pembungkus yang ingin Anda gunakan.

Dekripsi ciphertext dengan komitmen utama

Versi 1.7. x dapat mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen kunci. Namun, itu tidak dapat mengenkripsi ciphertext dengan komitmen utama. Properti ini

memungkinkan Anda untuk sepenuhnya menyebarkan aplikasi yang dapat mendekripsi ciphertext yang dienkripsi dengan komitmen utama sebelum mereka menemukan ciphertext semacam itu. Karena versi ini mendekripsi pesan yang dienkripsi tanpa komitmen utama, Anda tidak perlu mengenkripsi ulang ciphertext apa pun.

Untuk menerapkan perilaku ini, versi 1.7. x mencakup pengaturan konfigurasi kebijakan komitmen baru yang menentukan apakah AWS Encryption SDK dapat mengenkripsi atau mendekripsi dengan komitmen utama. Dalam versi 1.7. x, satu-satunya nilai yang valid untuk kebijakan komitmen,`ForbidEncryptAllowDecrypt`, digunakan dalam semua operasi enkripsi dan dekripsi. Nilai ini AWS Encryption SDK mencegah enkripsi dengan salah satu suite algoritme baru yang menyertakan komitmen utama. Hal ini memungkinkan AWS Encryption SDK untuk mendekripsi ciphertext dengan dan tanpa komitmen utama.

Meskipun hanya ada satu nilai kebijakan komitmen yang valid di versi 1.7. x, kami mengharuskan Anda untuk mengatur nilai ini secara eksplisit saat Anda menggunakan yang baru APIs diperkenalkan dalam rilis ini. Menyetel nilai secara eksplisit mencegah kebijakan komitmen Anda berubah secara otomatis menjadi `require-encrypt-require-decrypt` saat Anda meningkatkan ke versi 2.1. x. Sebagai gantinya, Anda dapat memigrasikan kebijakan komitmen Anda secara bertahap.

Suite algoritma dengan komitmen utama

Versi 1.7. x mencakup dua rangkaian algoritma baru yang mendukung komitmen utama. Satu termasuk penandatanganan; yang lain tidak. Seperti suite algoritma yang didukung sebelumnya, kedua suite algoritma baru ini mencakup enkripsi dengan AES-GCM, kunci enkripsi 256-bit, dan fungsi derivasi kunci berbasis HMAC (extract-and-expandHKDF).

Namun, rangkaian algoritma default yang digunakan untuk enkripsi tidak berubah. Suite algoritma ini ditambahkan ke versi 1.7. x untuk mempersiapkan aplikasi Anda untuk menggunakannya dalam versi 2.0. x dan kemudian.

Perubahan implementasi CMM

Versi 1.7. x memperkenalkan perubahan pada antarmuka Default cryptographic materials manager (CMM) untuk mendukung komitmen utama. Perubahan ini hanya memengaruhi Anda jika Anda telah menulis CMM khusus. Untuk detailnya, lihat dokumentasi API atau GitHub repositori untuk bahasa pemrograman Anda.

Versi 2.0. x

Versi 2.0. x mendukung fitur keamanan baru yang ditawarkan di AWS Encryption SDK, termasuk kunci pembungkus yang ditentukan dan komitmen utama. Untuk mendukung fitur-fitur ini, versi 2.0. x termasuk melanggar perubahan untuk versi sebelumnya dari file AWS Encryption SDK. Anda dapat mempersiapkan perubahan ini dengan menerapkan versi 1.7. x. Versi 2.0. x mencakup semua fitur baru yang diperkenalkan di versi 1.7. x dengan penambahan dan perubahan berikut.

> **Note**
>
> Versi 2. x. x dari AWS Encryption SDK for Python, AWS Encryption SDK for JavaScript, dan CLI AWS Enkripsi sedang dalam fase. end-of-support
> Untuk informasi tentang dukungan dan pemeliharaan AWS Encryption SDK versi ini dalam bahasa pemrograman pilihan Anda, lihat `SUPPORT_POLICY.rst` file di GitHubrepositorinya.

AWS KMS penyedia kunci master

Konstruktor penyedia kunci AWS KMS master asli yang tidak digunakan lagi di versi 1.7. x dihapus dalam versi 2.0. x. Anda harus secara eksplisit membangun penyedia kunci AWS KMS master dalam mode ketat atau mode penemuan.

Enkripsi dan dekripsi ciphertext dengan komitmen utama

Versi 2.0. x dapat mengenkripsi dan mendekripsi ciphertext dengan atau tanpa komitmen kunci. Perilakunya ditentukan oleh pengaturan kebijakan komitmen. Secara default, selalu mengenkripsi dengan komitmen utama dan hanya mendekripsi ciphertext yang dienkripsi dengan komitmen utama. Kecuali Anda mengubah kebijakan komitmen, ciphertext tidak AWS Encryption SDK akan mendekripsi ciphertext yang dienkripsi oleh versi sebelumnya, termasuk versi 1.7. AWS Encryption SDKx.

> **Important**
>
> Secara default, versi 2.0. x tidak akan mendekripsi ciphertext apa pun yang dienkripsi tanpa komitmen kunci. Jika aplikasi Anda mungkin menemukan ciphertext yang dienkripsi tanpa komitmen utama, tetapkan nilai kebijakan komitmen dengan. `AllowDecrypt`

Dalam versi 2.0. x, pengaturan kebijakan komitmen memiliki tiga nilai yang valid:

- `ForbidEncryptAllowDecrypt`— AWS Encryption SDK Tidak dapat mengenkripsi dengan komitmen utama. Ini dapat mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen utama.
- `RequireEncryptAllowDecrypt`— AWS Encryption SDK Harus dienkripsi dengan komitmen utama. Ini dapat mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen utama.
- `RequireEncryptRequireDecrypt`(default) — AWS Encryption SDK Harus dienkripsi dengan komitmen utama. Itu hanya mendekripsi ciphertext dengan komitmen utama.

Jika Anda bermigrasi dari versi sebelumnya AWS Encryption SDK ke versi 2.0. x, tetapkan kebijakan komitmen ke nilai yang memastikan bahwa Anda dapat mendekripsi semua ciphertext yang ada yang mungkin ditemui aplikasi Anda. Anda cenderung menyesuaikan pengaturan ini dari waktu ke waktu.

Versi 2.2. x

Menambahkan dukungan untuk tanda tangan digital dan membatasi kunci data terenkripsi.

> **Note**
>
> Versi 2. x. x dari AWS Encryption SDK for Python, AWS Encryption SDK for JavaScript, dan CLI AWS Enkripsi sedang dalam fase. end-of-support
> Untuk informasi tentang dukungan dan pemeliharaan AWS Encryption SDK versi ini dalam bahasa pemrograman pilihan Anda, lihat `SUPPORT_POLICY.rst` file di GitHubrepositorinya.

Tanda tangan digital

Untuk meningkatkan penanganan tanda tangan digital saat mendekripsi, AWS Encryption SDK termasuk fitur berikut:

- Mode non-streaming — mengembalikan teks biasa hanya setelah memproses semua input, termasuk memverifikasi tanda tangan digital jika ada. Fitur ini mencegah Anda menggunakan plaintext sebelum memverifikasi tanda tangan digital. Gunakan fitur ini setiap kali Anda mendekripsi data yang dienkripsi dengan tanda tangan digital (rangkaian algoritme default). Misalnya, karena CLI AWS Enkripsi selalu memproses data dalam mode streaming, gunakan `--buffer` parameter saat mendekripsi ciphertext dengan tanda tangan digital.
- Mode dekripsi khusus tanpa tanda tangan — fitur ini hanya mendekripsi ciphertext yang tidak ditandatangani. Jika dekripsi menemukan tanda tangan digital dalam ciphertext, operasi gagal.

Gunakan fitur ini untuk menghindari pemrosesan plaintext secara tidak sengaja dari pesan yang ditandatangani sebelum memverifikasi tanda tangan.

Membatasi kunci data terenkripsi

Anda dapat membatasi jumlah kunci data terenkripsi dalam pesan terenkripsi. Fitur ini dapat membantu Anda mendeteksi penyedia kunci master atau keyring yang salah konfigurasi saat mengenkripsi, atau mengidentifikasi ciphertext berbahaya saat mendekripsi.

Anda harus membatasi kunci data terenkripsi saat mendekripsi pesan dari sumber yang tidak tepercaya. Ini mencegah panggilan yang tidak perlu, mahal, dan berpotensi lengkap ke infrastruktur utama Anda.

Versi 2.3. x

Menambahkan dukungan untuk kunci AWS KMS Multi-wilayah. Lihat perinciannya di Menggunakan Multi-region AWS KMS keys.

> **Note**
>
> CLI AWS Enkripsi mendukung kunci Multi-wilayah yang dimulai pada versi 3.0. x.
> Versi 2. x. x dari AWS Encryption SDK for Python, AWS Encryption SDK for JavaScript, dan CLI AWS Enkripsi sedang dalam fase. end-of-support
> Untuk informasi tentang dukungan dan pemeliharaan AWS Encryption SDK versi ini dalam bahasa pemrograman pilihan Anda, lihat `SUPPORT_POLICY.rst` file di GitHubrepositorinya.

Migrasi Anda AWS Encryption SDK

AWS Encryption SDK Mendukung beberapa implementasi bahasa pemrograman interoperable, yang masing-masing dikembangkan dalam repositori open-source pada. GitHub Sebagai praktik terbaik, kami menyarankan Anda menggunakan versi terbaru AWS Encryption SDK untuk setiap bahasa.

Anda dapat meng-upgrade dengan aman dari versi 2.0. x atau yang lebih baru AWS Encryption SDK ke versi terbaru. Namun, 2.0. versi x AWS Encryption SDK memperkenalkan fitur keamanan baru yang signifikan, beberapa di antaranya melanggar perubahan. Untuk meng-upgrade dari versi lebih awal dari 1.7. x ke versi 2.0. x dan yang lebih baru, Anda harus terlebih dahulu meningkatkan ke yang terbaru 1. versi x. Topik di bagian ini dirancang untuk membantu Anda memahami perubahan, memilih versi yang benar untuk aplikasi Anda, dan bermigrasi dengan aman dan berhasil ke versi terbaru. AWS Encryption SDK

Untuk informasi tentang versi signifikan dari AWS Encryption SDK, lihatVersi dari AWS Encryption SDK.

Important

Jangan meng-upgrade langsung dari versi yang lebih awal dari 1.7. x ke versi 2.0. x atau yang lebih baru tanpa terlebih dahulu meningkatkan ke yang terbaru 1. versi x. Jika Anda meng-upgrade langsung ke versi 2.0. x atau yang lebih baru dan mengaktifkan semua fitur baru dengan segera, tidak AWS Encryption SDK akan dapat mendekripsi ciphertext yang dienkripsi di bawah versi yang lebih lama. AWS Encryption SDK

Note

Versi paling awal AWS Encryption SDK untuk .NET adalah versi 3.0. x. Semua versi AWS Encryption SDK untuk .NET mendukung praktik terbaik keamanan yang diperkenalkan di 2.0. x dari AWS Encryption SDK. Anda dapat dengan aman meningkatkan ke versi terbaru tanpa kode atau perubahan data.

AWS Enkripsi CLI: Saat membaca panduan migrasi ini, gunakan 1.7. x instruksi migrasi untuk AWS Enkripsi CLI 1.8. x dan gunakan 2.0. x instruksi migrasi untuk AWS Enkripsi CLI 2.1. x. Lihat perinciannya di Versi CLI AWS Enkripsi.

Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x

menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Pengguna baru

Jika Anda baru mengenal AWS Encryption SDK, instal versi terbaru AWS Encryption SDK untuk bahasa pemrograman Anda. Nilai default memungkinkan semua fitur keamanan AWS Encryption SDK, termasuk enkripsi dengan penandatanganan, derivasi kunci, dan komitmen utama. AWS Encryption SDK

Pengguna saat ini

Kami menyarankan Anda meningkatkan dari versi Anda saat ini ke versi terbaru yang tersedia sesegera mungkin. Semua 1. x versi AWS Encryption SDK berada dalam end-of-support fase, seperti versi yang lebih baru dalam beberapa bahasa pemrograman. Untuk detail tentang status dukungan dan pemeliharaan AWS Encryption SDK dalam bahasa pemrograman Anda, lihatSupport dan pemeliharaan.

AWS Encryption SDK versi 2.0. x dan yang lebih baru menyediakan fitur keamanan baru untuk membantu melindungi data Anda. Namun, AWS Encryption SDK versi 2.0. x termasuk melanggar perubahan yang tidak kompatibel ke belakang. Untuk memastikan transisi yang aman, mulailah dengan bermigrasi dari versi Anda saat ini ke versi terbaru 1. x dalam bahasa pemrograman Anda. Ketika terbaru Anda 1. versi x sepenuhnya digunakan dan beroperasi dengan sukses, Anda dapat dengan aman bermigrasi ke versi 2.0. x dan kemudian. Proses dua langkah ini sangat penting terutama untuk aplikasi terdistribusi.

Untuk informasi selengkapnya tentang fitur AWS Encryption SDK keamanan yang mendasari perubahan ini, lihat Peningkatan enkripsi sisi klien: Komitmen eksplisit KeyIds dan kunci di Blog Keamanan.AWS

Mencari bantuan dengan menggunakan AWS Encryption SDK for Java dengan AWS SDK for Java 2.x? Lihat Prasyarat.

Topik

- Cara memigrasi dan menyebarkan AWS Encryption SDK
- Memperbarui penyedia kunci AWS KMS utama
- Memperbarui AWS KMS keyrings

- Menetapkan kebijakan komitmen Anda
- Memecahkan masalah migrasi ke versi terbaru

Cara memigrasi dan menyebarkan AWS Encryption SDK

Saat bermigrasi dari AWS Encryption SDK versi lebih awal dari 1.7. x ke versi 2.0. x atau yang lebih baru, Anda harus bertransisi dengan aman ke enkripsi dengan komitmen utama. Jika tidak, aplikasi Anda akan menemukan ciphertext yang tidak dapat didekripsi. Jika Anda menggunakan penyedia kunci AWS KMS master, Anda harus memperbarui ke konstruktor baru yang membuat penyedia kunci master dalam mode ketat atau mode penemuan.

> **Note**
>
> Topik ini dirancang untuk pengguna yang bermigrasi dari versi sebelumnya AWS Encryption SDK ke versi 2.0. x atau yang lebih baru. Jika Anda baru mengenal AWS Encryption SDK, Anda dapat mulai menggunakan versi terbaru yang tersedia segera dengan pengaturan default.

Untuk menghindari situasi kritis di mana Anda tidak dapat mendekripsi ciphertext yang perlu Anda baca, sebaiknya Anda bermigrasi dan menerapkan dalam beberapa tahap berbeda. Verifikasi bahwa setiap tahap selesai dan sepenuhnya digunakan sebelum memulai tahap berikutnya. Ini sangat penting untuk aplikasi terdistribusi dengan banyak host.

Tahap 1: Perbarui aplikasi Anda ke yang terbaru 1. versi x

Perbarui ke yang terbaru 1. versi x untuk bahasa pemrograman Anda. Uji dengan seksama, terapkan perubahan Anda, dan konfirmasikan bahwa pembaruan telah disebarkan ke semua host tujuan sebelum memulai tahap 2.

> **Important**
>
> Verifikasi bahwa terbaru Anda 1. Versi x adalah versi 1.7. x atau yang lebih baru AWS Encryption SDK.

Yang terbaru 1. versi x AWS Encryption SDK kompatibel dengan versi lama AWS Encryption SDK dan maju yang kompatibel dengan versi 2.0. x dan kemudian. Mereka termasuk fitur-fitur baru

yang hadir di versi 2.0. x, tetapi sertakan default aman yang dirancang untuk migrasi ini. Mereka memungkinkan Anda untuk meng-upgrade penyedia kunci AWS KMS master Anda, jika perlu, dan untuk sepenuhnya menyebarkan dengan suite algoritma yang dapat mendekripsi ciphertext dengan komitmen utama.

- Ganti elemen usang, termasuk konstruktor untuk penyedia kunci master lama AWS KMS . Dengan Python, pastikan untuk mengaktifkan peringatan penghentian. Elemen kode yang tidak digunakan lagi di 1 terbaru. versi x dihapus dari versi 2.0. x dan kemudian.
- Tetapkan kebijakan komitmen Anda secara eksplisit. `ForbidEncryptAllowDecrypt` Meskipun ini adalah satu-satunya nilai yang valid di 1 terbaru. x versi, pengaturan ini diperlukan saat Anda menggunakan yang APIs diperkenalkan dalam rilis ini. Ini mencegah aplikasi Anda menolak ciphertext yang dienkripsi tanpa komitmen utama saat Anda bermigrasi ke versi 2.0. x dan kemudian. Lihat perinciannya di the section called “Menetapkan kebijakan komitmen Anda”.
- Jika Anda menggunakan penyedia kunci AWS KMS master, Anda harus memperbarui penyedia kunci master lama Anda untuk menguasai penyedia kunci yang mendukung mode ketat dan mode penemuan. Pembaruan ini diperlukan untuk AWS Encryption SDK for Java, AWS Encryption SDK for Python, dan CLI AWS Enkripsi. Jika Anda menggunakan penyedia kunci utama dalam mode penemuan, sebaiknya Anda menerapkan filter penemuan yang membatasi kunci pembungkus yang digunakan untuk kunci tertentu Akun AWS. Pembaruan ini opsional, tetapi ini adalah praktik terbaik yang kami rekomendasikan. Lihat perinciannya di Memperbarui penyedia kunci AWS KMS utama.
- Jika Anda menggunakan cincin kunci AWS KMS penemuan, sebaiknya sertakan filter penemuan yang membatasi kunci pembungkus yang digunakan dalam dekripsi pada kunci tertentu. Akun AWS Pembaruan ini opsional, tetapi ini adalah praktik terbaik yang kami rekomendasikan. Lihat perinciannya di Memperbarui AWS KMS keyrings.

Tahap 2: Perbarui aplikasi Anda ke versi terbaru

Setelah menerapkan yang terbaru 1. x versi berhasil untuk semua host, Anda dapat meng-upgrade ke versi 2.0. x dan kemudian. Versi 2.0. x termasuk melanggar perubahan untuk semua versi sebelumnya dari file AWS Encryption SDK. Namun, jika Anda membuat perubahan kode yang direkomendasikan di Tahap 1, Anda dapat menghindari kesalahan saat bermigrasi ke versi terbaru.

Sebelum Anda memperbarui ke versi terbaru, verifikasi bahwa kebijakan komitmen Anda diatur secara konsisten`ForbidEncryptAllowDecrypt`. Kemudian, tergantung pada konfigurasi data Anda, Anda dapat bermigrasi dengan kecepatan Anda sendiri ke `RequireEncryptAllowDecrypt`

dan kemudian ke pengaturan default,`RequireEncryptRequireDecrypt`. Kami merekomendasikan serangkaian langkah transisi seperti pola berikut.

1. Mulailah dengan kebijakan komitmen Anda yang ditetapkan`ForbidEncryptAllowDecrypt`. AWS Encryption SDK Dapat mendekripsi pesan dengan komitmen utama, tetapi belum mengenkripsi dengan komitmen utama.
2. Ketika Anda siap, perbarui kebijakan komitmen Anda untuk`RequireEncryptAllowDecrypt`. AWS Encryption SDK Mulai mengenkripsi data Anda dengan komitmen utama. Itu dapat mendekripsi ciphertext dengan dan tanpa komitmen utama.

   Sebelum memperbarui kebijakan komitmen Anda`RequireEncryptAllowDecrypt`, verifikasi bahwa kebijakan terbaru Anda 1. Versi x digunakan untuk semua host, termasuk host dari aplikasi apa pun yang mendekripsi ciphertext yang Anda hasilkan. Versi AWS Encryption SDK sebelumnya ke versi 1.7. x tidak dapat mendekripsi pesan yang dienkripsi dengan komitmen utama.

   Ini juga saat yang tepat untuk menambahkan metrik ke aplikasi Anda untuk mengukur apakah Anda masih memproses ciphertext tanpa komitmen utama. Ini akan membantu Anda menentukan kapan aman untuk memperbarui pengaturan kebijakan komitmen Anda`RequireEncryptRequireDecrypt`. Untuk beberapa aplikasi, seperti yang mengenkripsi pesan dalam antrian Amazon SQS, ini mungkin berarti menunggu cukup lama sehingga semua ciphertext yang dienkripsi di bawah versi lama telah dienkripsi ulang atau dihapus. Untuk aplikasi lain, seperti objek S3 terenkripsi, Anda mungkin perlu mengunduh, mengenkripsi ulang, dan mengunggah ulang semua objek.
3. Ketika Anda yakin bahwa Anda tidak memiliki pesan yang dienkripsi tanpa komitmen utama, Anda dapat memperbarui kebijakan komitmen Anda. `RequireEncryptRequireDecrypt` Nilai ini memastikan bahwa data Anda selalu dienkripsi dan didekripsi dengan komitmen utama. Pengaturan ini adalah default, jadi Anda tidak diharuskan untuk mengaturnya secara eksplisit, tetapi kami merekomendasikannya. Pengaturan eksplisit akan membantu debugging dan potensi rollback yang mungkin diperlukan jika aplikasi Anda menemukan ciphertext yang dienkripsi tanpa komitmen utama.

Memperbarui penyedia kunci AWS KMS utama

Untuk bermigrasi ke yang terbaru 1. x versi AWS Encryption SDK, dan kemudian ke versi 2.0. x atau yang lebih baru, Anda harus mengganti penyedia kunci AWS KMS master lama dengan penyedia kunci master yang dibuat secara eksplisit dalam mode ketat atau mode penemuan. Penyedia kunci master lama tidak digunakan lagi di versi 1.7. x dan dihapus dalam versi 2.0. x. Perubahan

ini diperlukan untuk aplikasi dan skrip yang menggunakan AWS Encryption SDK for Java, AWS Encryption SDK for Python, dan CLI AWS Enkripsi. Contoh di bagian ini akan menunjukkan cara memperbarui kode Anda.

> **Note**
>
> Dengan Python, aktifkan peringatan penghentian. Ini akan membantu Anda mengidentifikasi bagian-bagian kode Anda yang perlu Anda perbarui.

Jika Anda menggunakan kunci AWS KMS master (bukan penyedia kunci master), Anda dapat melewati langkah ini. AWS KMS kunci master tidak digunakan lagi atau dihapus. Mereka mengenkripsi dan mendekripsi hanya dengan kunci pembungkus yang Anda tentukan.

Contoh di bagian ini berfokus pada elemen kode Anda yang perlu Anda ubah. Untuk contoh lengkap kode yang diperbarui, lihat bagian Contoh GitHub repositori untuk bahasa pemrograman Anda. Juga, contoh-contoh ini biasanya menggunakan kunci ARNs untuk mewakili AWS KMS keys. Saat Anda membuat penyedia kunci utama untuk mengenkripsi, Anda dapat menggunakan pengidentifikasi AWS KMS kunci yang valid untuk mewakili. AWS KMS key Saat Anda membuat penyedia kunci master untuk mendekripsi, Anda harus menggunakan ARN kunci.

Pelajari lebih lanjut tentang migrasi

Untuk semua AWS Encryption SDK pengguna, pelajari tentang menetapkan kebijakan komitmen Andathe section called “Menetapkan kebijakan komitmen Anda”.

Untuk AWS Encryption SDK for C dan AWS Encryption SDK for JavaScript pengguna, pelajari tentang pembaruan opsional untuk keyrings diMemperbarui AWS KMS keyrings.

Topik

- Migrasi ke mode ketat
- Migrasi ke mode penemuan

Migrasi ke mode ketat

Setelah memperbarui ke yang terbaru 1. x versi AWS Encryption SDK, ganti penyedia kunci master lama Anda dengan penyedia kunci master dalam mode ketat. Dalam mode ketat, Anda harus menentukan kunci pembungkus yang akan digunakan saat mengenkripsi dan mendekripsi. Hanya

AWS Encryption SDK menggunakan tombol pembungkus yang Anda tentukan. Penyedia kunci master yang tidak digunakan lagi dapat mendekripsi data menggunakan data apa pun AWS KMS key yang mengenkripsi kunci data, termasuk di berbagai dan Wilayah. AWS KMS keys Akun AWS

Penyedia kunci utama dalam mode ketat diperkenalkan dalam AWS Encryption SDK versi 1.7. x. Mereka menggantikan penyedia kunci master lama, yang tidak digunakan lagi di 1.7. x dan dihapus di 2.0. x. Menggunakan penyedia kunci master dalam mode ketat adalah praktik AWS Encryption SDK terbaik.

Kode berikut membuat penyedia kunci master dalam mode ketat yang dapat Anda gunakan untuk mengenkripsi dan mendekripsi.

Java

Contoh ini mewakili kode dalam aplikasi yang menggunakan versi 1.6.2 atau sebelumnya. AWS Encryption SDK for Java

Kode ini menggunakan `KmsMasterKeyProvider.builder()` metode untuk membuat instance penyedia kunci AWS KMS master yang menggunakannya AWS KMS key sebagai kunci pembungkus.

```
// Create a master key provider
// Replace the example key ARN with a valid one
String awsKmsKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

KmsMasterKeyProvider masterKeyProvider = KmsMasterKeyProvider.builder()
    .withKeysForEncryption(awsKmsKey)
    .build();
```

Contoh ini mewakili kode dalam aplikasi yang menggunakan versi 1.7. x atau yang lebih baru AWS Encryption SDK for Java . Untuk contoh lengkap, lihat BasicEncryptionExample.java.

`Builder.withKeysForEncryption()`Metode `Builder.build()` dan yang digunakan dalam contoh sebelumnya tidak digunakan lagi di versi 1.7. x dan dihapus dari versi 2.0. x.

Untuk memperbarui ke penyedia kunci master mode ketat, kode ini menggantikan panggilan ke metode usang dengan panggilan ke metode baru. `Builder.buildStrict()` Contoh ini menentukan satu AWS KMS key sebagai kunci pembungkus, tetapi `Builder.buildStrict()` metode ini dapat mengambil daftar beberapa. AWS KMS keys

```
// Create a master key provider in strict mode
// Replace the example key ARN with a valid one from your Akun AWS.
String awsKmsKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

KmsMasterKeyProvider masterKeyProvider = KmsMasterKeyProvider.builder()
    .buildStrict(awsKmsKey);
```

Python

Contoh ini mewakili kode dalam aplikasi yang menggunakan versi 1.4.1 dari file. AWS Encryption SDK for Python Kode ini menggunakan`KMSMasterKeyProvider`, yang tidak digunakan lagi di versi 1.7. x dan dihapus dari versi 2.0. x. Saat mendekripsi, ia menggunakan apa pun AWS KMS key yang mengenkripsi kunci data tanpa memperhatikan yang Anda tentukan. AWS KMS keys

Perhatikan bahwa `KMSMasterKey` tidak digunakan lagi atau dihapus. Saat mengenkripsi dan mendekripsi, hanya menggunakan yang Anda tentukan. AWS KMS key

```
# Create a master key provider
# Replace the example key ARN with a valid one
key_1 = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
key_2 = "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"

aws_kms_master_key_provider = KMSMasterKeyProvider(
   key_ids=[key_1, key_2]
)
```

Contoh ini mewakili kode dalam aplikasi yang menggunakan versi 1.7. x dari AWS Encryption SDK for Python. Untuk contoh lengkap, lihat basic_encryption.py.

Untuk memperbarui ke penyedia kunci master mode ketat, kode ini menggantikan panggilan ke `KMSMasterKeyProvider()` dengan panggilan ke`StrictAwsKmsMasterKeyProvider()`.

```
# Create a master key provider in strict mode
# Replace the example key ARNs with valid values from your Akun AWS
key_1 = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
key_2 = "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
```

```
aws_kms_master_key_provider = StrictAwsKmsMasterKeyProvider(
    key_ids=[key_1, key_2]
)
```

AWS Encryption CLI

Contoh ini menunjukkan cara mengenkripsi dan mendekripsi menggunakan Enkripsi AWS CLI versi 1.1.7 atau sebelumnya.

Di versi 1.1.7 dan sebelumnya, saat mengenkripsi, Anda menentukan satu atau lebih kunci master (atau kunci pembungkus), seperti. AWS KMS key Saat mendekripsi, Anda tidak dapat menentukan kunci pembungkus apa pun kecuali Anda menggunakan penyedia kunci master khusus. CLI AWS Enkripsi dapat menggunakan kunci pembungkus apa pun yang mengenkripsi kunci data.

```
\\ Replace the example key ARN with a valid one
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

\\ Encrypt your plaintext data
$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --master-keys key=$keyArn \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --output .

\\ Decrypt your ciphertext
$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --output .
```

Contoh ini menunjukkan cara mengenkripsi dan mendekripsi menggunakan Enkripsi AWS CLI versi 1.7. x atau yang lebih baru. Untuk contoh lengkap, lihatContoh CLI AWS Enkripsi.

`--master-keys`Parameter ini tidak digunakan lagi di versi 1.7. x dan dihapus dalam versi 2.0. x. Ini diganti dengan `--wrapping-keys` parameter, yang diperlukan dalam perintah enkripsi dan dekripsi. Parameter ini mendukung mode ketat dan mode penemuan. Mode ketat adalah praktik AWS Encryption SDK terbaik yang memastikan bahwa Anda menggunakan kunci pembungkus yang Anda inginkan.

Untuk meningkatkan ke mode ketat, gunakan atribut kunci `--wrapping-keys` parameter untuk menentukan kunci pembungkus saat mengenkripsi dan mendekripsi.

```
\\ Replace the example key ARN with a valid value
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

\\ Encrypt your plaintext data
$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --wrapping-keys key=$keyArn \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --output .

\\ Decrypt your ciphertext
$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys key=$keyArn \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --output .
```

Migrasi ke mode penemuan

Dimulai pada versi 1.7. x, ini adalah praktik AWS Encryption SDK terbaik untuk menggunakan mode ketat untuk penyedia kunci AWS KMS master, yaitu menentukan kunci pembungkus saat mengenkripsi dan mendekripsi. Anda harus selalu menentukan kunci pembungkus saat mengenkripsi. Tetapi ada situasi di mana menentukan kunci ARNs AWS KMS keys untuk mendekripsi tidak praktis. Misalnya, jika Anda menggunakan alias untuk mengidentifikasi AWS KMS keys saat mengenkripsi, Anda kehilangan manfaat alias jika Anda harus mencantumkan kunci saat mendekripsi. ARNs Selain itu, karena penyedia kunci master dalam mode penemuan berperilaku seperti penyedia kunci master asli, Anda dapat menggunakannya sementara sebagai bagian dari strategi migrasi Anda, dan kemudian meningkatkan ke penyedia kunci master dalam mode ketat nanti.

Dalam kasus seperti ini, Anda dapat menggunakan penyedia kunci utama dalam mode penemuan. Penyedia kunci master ini tidak mengizinkan Anda menentukan kunci pembungkus, sehingga Anda tidak dapat menggunakannya untuk mengenkripsi. Saat mendekripsi, mereka dapat menggunakan kunci pembungkus apa pun yang mengenkripsi kunci data. Tetapi tidak seperti penyedia kunci

master lama, yang berperilaku dengan cara yang sama, Anda membuatnya dalam mode penemuan secara eksplisit. Saat menggunakan penyedia kunci master dalam mode penemuan, Anda dapat membatasi kunci pembungkus yang dapat digunakan untuk yang khusus Akun AWS. Filter penemuan ini opsional, tetapi ini adalah praktik terbaik yang kami rekomendasikan. Untuk informasi tentang AWS partisi dan akun, lihat Nama Sumber Daya Amazon di bagian. Referensi Umum AWS

Contoh berikut membuat penyedia kunci AWS KMS master dalam mode ketat untuk mengenkripsi dan penyedia kunci AWS KMS master dalam mode penemuan untuk mendekripsi. Penyedia kunci master dalam mode penemuan menggunakan filter penemuan untuk membatasi kunci pembungkus yang digunakan untuk mendekripsi ke `aws` partisi dan contoh tertentu. Akun AWS Meskipun filter akun tidak diperlukan dalam contoh yang sangat sederhana ini, ini adalah praktik terbaik yang sangat bermanfaat ketika satu aplikasi mengenkripsi data dan aplikasi lain mendekripsi data.

Java

Contoh ini mewakili kode dalam aplikasi yang menggunakan versi 1.7. x atau yang lebih baru AWS Encryption SDK for Java. Untuk contoh lengkap, lihat DiscoveryDecryptionExample.java.

Untuk membuat instance penyedia kunci master dalam mode ketat untuk mengenkripsi, contoh ini menggunakan metode ini. `Builder.buildStrict()` Untuk membuat instance penyedia kunci master dalam mode penemuan untuk mendekripsi, ia menggunakan metode ini. `Builder.buildDiscovery()` `Builder.buildDiscovery()`Metode ini mengambil `DiscoveryFilter` yang membatasi AWS Encryption SDK ke AWS KMS keys dalam AWS partisi dan akun yang ditentukan.

```
// Create a master key provider in strict mode for encrypting
// Replace the example alias ARN with a valid one from your Akun AWS.
String awsKmsKey = "arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias";

KmsMasterKeyProvider encryptingKeyProvider = KmsMasterKeyProvider.builder()
    .buildStrict(awsKmsKey);

// Create a master key provider in discovery mode for decrypting
// Replace the example account IDs with valid values.
DiscoveryFilter accounts = new DiscoveryFilter("aws", Arrays.asList("111122223333",
 "444455556666"));

KmsMasterKeyProvider decryptingKeyProvider = KmsMasterKeyProvider.builder()
    .buildDiscovery(accounts);
```

Python

Contoh ini mewakili kode dalam aplikasi yang menggunakan versi 1.7. x atau yang lebih baru AWS Encryption SDK for Python . Untuk contoh lengkap, lihat discovery_kms_provider.py.

Untuk membuat penyedia kunci master dalam mode ketat untuk mengenkripsi, contoh ini menggunakan. `StrictAwsKmsMasterKeyProvider` Untuk membuat penyedia kunci master dalam mode penemuan untuk mendekripsi, ia menggunakan `DiscoveryAwsKmsMasterKeyProvider` dengan a `DiscoveryFilter` yang membatasi AWS Encryption SDK ke AWS KMS keys dalam AWS partisi dan akun yang ditentukan.

```
# Create a master key provider in strict mode
# Replace the example key ARN and alias ARNs with valid values from your Akun AWS.
key_1 = "arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias"
key_2 = "arn:aws:kms:us-
west-2:444455556666:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"

aws_kms_master_key_provider = StrictAwsKmsMasterKeyProvider(
    key_ids=[key_1, key_2]
)

# Create a master key provider in discovery mode for decrypting
# Replace the example account IDs with valid values
accounts = DiscoveryFilter(
    partition="aws",
    account_ids=["111122223333", "444455556666"]
)
aws_kms_master_key_provider = DiscoveryAwsKmsMasterKeyProvider(
        discovery_filter=accounts
)
```

AWS Encryption CLI

Contoh ini menunjukkan cara mengenkripsi dan mendekripsi menggunakan Enkripsi AWS CLI versi 1.7. x atau yang lebih baru. Dimulai pada versi 1.7. x, `--wrapping-keys` parameter diperlukan saat mengenkripsi dan mendekripsi. `--wrapping-keys`Parameter mendukung mode ketat dan mode penemuan. Untuk contoh lengkap, lihatthe section called “Contoh”.

Saat mengenkripsi, contoh ini menentukan kunci pembungkus, yang diperlukan. Saat mendekripsi, secara eksplisit memilih mode penemuan dengan menggunakan `discovery` atribut `--wrapping-keys` parameter dengan nilai. `true`

Untuk membatasi kunci pembungkus yang AWS Encryption SDK dapat digunakan dalam mode penemuan pada khususnya Akun AWS, contoh ini menggunakan `discovery-account` atribut `discovery-partition` dan `--wrapping-keys` parameter. Atribut opsional ini hanya valid ketika `discovery` atribut diatur ke`true`. Anda harus menggunakan `discovery-account` atribut `discovery-partition` dan bersama-sama; tidak ada yang valid sendirian.

```
\\ Replace the example key ARN with a valid value
$ keyAlias=arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias

\\ Encrypt your plaintext data
$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --wrapping-keys key=$keyAlias \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --output .

\\ Decrypt your ciphertext
\\ Replace the example account IDs with valid values
$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys discovery=true \
                                     discovery-partition=aws \
                                     discovery-account=111122223333 \
                                     discovery-account=444455556666 \
                     --encryption-context purpose=test \
                     --metadata-output ~/metadata \
                     --output .
```

Memperbarui AWS KMS keyrings

AWS KMS Gantungan kunci di AWS Encryption SDK for C, AWS Encryption SDK untuk .NET, dan AWS Encryption SDK for JavaScriptmendukung praktik terbaik dengan memungkinkan Anda menentukan kunci pembungkus saat mengenkripsi dan mendekripsi. Jika Anda membuat keyring AWS KMS penemuan, Anda melakukannya secara eksplisit.

> **Note**
>
> Versi paling awal AWS Encryption SDK untuk .NET adalah versi 3.0. x. Semua versi AWS Encryption SDK untuk .NET mendukung praktik terbaik keamanan yang diperkenalkan di 2.0.

x dari AWS Encryption SDK. Anda dapat dengan aman meningkatkan ke versi terbaru tanpa kode atau perubahan data.

Saat Anda memperbarui ke yang terbaru 1. x versi AWS Encryption SDK, Anda dapat menggunakan filter penemuan untuk membatasi kunci pembungkus yang digunakan oleh keyring AWS KMS penemuan atau keyring penemuan AWS KMS regional saat mendekripsi ke kunci tertentu. Akun AWS Memfilter keyring penemuan adalah praktik AWS Encryption SDK terbaik.

Contoh di bagian ini akan menunjukkan cara menambahkan filter penemuan ke keyring penemuan AWS KMS regional.

Pelajari lebih lanjut tentang migrasi

Untuk semua AWS Encryption SDK pengguna, pelajari tentang menetapkan kebijakan komitmen Andathe section called “Menetapkan kebijakan komitmen Anda”.

Untuk AWS Encryption SDK for Java, AWS Encryption SDK for Python, dan pengguna CLI AWS Enkripsi, pelajari tentang pembaruan yang diperlukan untuk menguasai penyedia kunci di. the section called “Memperbarui penyedia kunci AWS KMS utama”

Anda mungkin memiliki kode seperti berikut dalam aplikasi Anda. Contoh ini membuat keyring penemuan AWS KMS regional yang hanya dapat menggunakan kunci pembungkus di Wilayah AS Barat (Oregon) (us-west-2). Contoh ini mewakili kode dalam AWS Encryption SDK versi lebih awal dari 1.7. x. Namun, ini masih berlaku di versi 1.7. x dan kemudian.

C

```
struct aws_cryptosdk_keyring *kms_regional_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder()
       .WithKmsClient(create_kms_client(Aws::Region::US_WEST_2)).BuildDiscovery());
```

JavaScript Browser

```
const clientProvider = getClient(KMS, { credentials })

const discovery = true
```

```
const clientProvider = limitRegions(['us-west-2'], getKmsClient)
const keyring = new KmsKeyringBrowser({ clientProvider, discovery })
```

JavaScript Node.js

```
const discovery = true
const clientProvider = limitRegions(['us-west-2'], getKmsClient)
const keyring = new KmsKeyringNode({ clientProvider, discovery })
```

Dimulai pada versi 1.7. x, Anda dapat menambahkan filter penemuan ke keyring AWS KMS penemuan apa pun. Filter penemuan ini membatasi AWS KMS keys yang AWS Encryption SDK dapat digunakan untuk dekripsi ke partisi dan akun yang ditentukan. Sebelum menggunakan kode ini, ubah partisi, jika perlu, dan ganti akun contoh IDs dengan yang valid.

C

Untuk contoh lengkap, lihat kms_discovery.cpp.

```
std::shared_ptr<KmsKeyring::DiscoveryFilter> discovery_filter(
    KmsKeyring::DiscoveryFilter::Builder("aws")
        .AddAccount("111122223333")
        .AddAccount("444455556666")
        .Build());

struct aws_cryptosdk_keyring *kms_regional_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder()

 .WithKmsClient(create_kms_client(Aws::Region::US_WEST_2)).BuildDiscovery(discovery_filter))
```

JavaScript Browser

```
const clientProvider = getClient(KMS, { credentials })

const discovery = true
const clientProvider = limitRegions(['us-west-2'], getKmsClient)
const keyring = new KmsKeyringBrowser(clientProvider, {
    discovery,
    discoveryFilter: { accountIDs: ['111122223333', '444455556666'], partition:
 'aws' }
})
```

JavaScript Node.js

Untuk contoh lengkap, lihat kms_filtered_discovery.ts.

```
const discovery = true
const clientProvider = limitRegions(['us-west-2'], getKmsClient)
const keyring = new KmsKeyringNode({
    clientProvider,
    discovery,
    discoveryFilter: { accountIDs: ['111122223333', '444455556666'], partition:
 'aws' }
})
```

Menetapkan kebijakan komitmen Anda

Komitmen utama memastikan bahwa data terenkripsi Anda selalu didekripsi ke teks biasa yang sama. Untuk menyediakan properti keamanan ini, dimulai dari versi 1.7. x, AWS Encryption SDK menggunakan suite algoritma baru dengan komitmen utama. Untuk menentukan apakah data Anda dienkripsi dan didekripsi dengan komitmen utama, gunakan pengaturan konfigurasi kebijakan komitmen. Mengenkripsi dan mendekripsi data dengan komitmen utama adalah praktik terbaik.AWS Encryption SDK

Menetapkan kebijakan komitmen adalah bagian penting dari langkah kedua dalam proses migrasi — migrasi dari yang terbaru 1. x versi AWS Encryption SDK ke versi 2.0. x dan kemudian. Setelah menetapkan dan mengubah kebijakan komitmen Anda, pastikan untuk menguji aplikasi Anda secara menyeluruh sebelum menerapkannya dalam produksi. Untuk panduan migrasi, lihatCara memigrasi dan menyebarkan AWS Encryption SDK.

Pengaturan kebijakan komitmen memiliki tiga nilai valid di versi 2.0. x dan kemudian. Yang terbaru 1. x versi (dimulai dengan versi 1.7. x), `ForbidEncryptAllowDecrypt` hanya valid.

- `ForbidEncryptAllowDecrypt`— AWS Encryption SDK Tidak dapat mengenkripsi dengan komitmen utama. Ini dapat mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen utama.

  Yang terbaru 1. x versi, ini adalah satu-satunya nilai yang valid. Ini memastikan bahwa Anda tidak mengenkripsi dengan komitmen utama sampai Anda sepenuhnya siap untuk mendekripsi dengan komitmen utama. Menyetel nilai secara eksplisit mencegah kebijakan komitmen Anda berubah secara otomatis menjadi `require-encrypt-require-decrypt` saat Anda meningkatkan ke

versi 2.0. x atau yang lebih baru. Sebagai gantinya, Anda dapat memigrasikan kebijakan komitmen Anda secara bertahap.

- `RequireEncryptAllowDecrypt`— AWS Encryption SDK Selalu dienkripsi dengan komitmen utama. Ini dapat mendekripsi ciphertext yang dienkripsi dengan atau tanpa komitmen utama. Nilai ini ditambahkan dalam versi 2.0. x.
- `RequireEncryptRequireDecrypt`— AWS Encryption SDK Selalu mengenkripsi dan mendekripsi dengan komitmen utama. Nilai ini ditambahkan dalam versi 2.0. x. Ini adalah nilai default dalam versi 2.0. x dan kemudian.

Yang terbaru 1. x versi, satu-satunya nilai kebijakan komitmen yang valid adalah`ForbidEncryptAllowDecrypt`. Setelah Anda bermigrasi ke versi 2.0. x atau lebih baru, Anda dapat mengubah kebijakan komitmen Anda secara bertahap saat Anda siap. Jangan perbarui kebijakan komitmen Anda `RequireEncryptRequireDecrypt` sampai Anda yakin bahwa Anda tidak memiliki pesan yang dienkripsi tanpa komitmen utama.

Contoh-contoh ini menunjukkan kepada Anda cara menetapkan kebijakan komitmen Anda di 1 terbaru. x versi dan dalam versi 2.0. x dan kemudian. Tekniknya tergantung pada bahasa pemrograman Anda.

Pelajari lebih lanjut tentang migrasi

Untuk AWS Encryption SDK for Java, AWS Encryption SDK for Python, dan CLI AWS Enkripsi, pelajari tentang perubahan yang diperlukan untuk menguasai penyedia kunci di. the section called “Memperbarui penyedia kunci AWS KMS utama”

Untuk AWS Encryption SDK for C dan AWS Encryption SDK for JavaScript, pelajari tentang pembaruan opsional untuk keyrings diMemperbarui AWS KMS keyrings.

Cara menetapkan kebijakan komitmen Anda

Teknik yang Anda gunakan untuk menetapkan kebijakan komitmen Anda sedikit berbeda dengan setiap implementasi bahasa. Contoh-contoh ini menunjukkan kepada Anda bagaimana melakukannya. Sebelum mengubah kebijakan komitmen Anda, tinjau pendekatan multi-tahap diCara bermigrasi dan menyebarkan.

C

Dimulai pada versi 1.7. x dari AWS Encryption SDK for C, Anda menggunakan `aws_cryptosdk_session_set_commitment_policy` fungsi untuk mengatur kebijakan

komitmen pada sesi enkripsi dan dekripsi Anda. Kebijakan komitmen yang Anda tetapkan berlaku untuk semua operasi enkripsi dan dekripsi yang dipanggil pada sesi tersebut.

`aws_cryptosdk_session_new_from_cmm`Fungsi `aws_cryptosdk_session_new_from_keyring` dan tidak digunakan lagi di versi 1.7. x dan dihapus dalam versi 2.0. x. Fungsi-fungsi ini digantikan oleh `aws_cryptosdk_session_new_from_keyring_2` dan `aws_cryptosdk_session_new_from_cmm_2` fungsi yang mengembalikan sesi.

Saat Anda menggunakan `aws_cryptosdk_session_new_from_keyring_2` dan `aws_cryptosdk_session_new_from_cmm_2` yang terbaru 1. x versi, Anda diminta untuk memanggil `aws_cryptosdk_session_set_commitment_policy` fungsi dengan nilai kebijakan `COMMITMENT_POLICY_FORBID_ENCRYPT_ALLOW_DECRYPT` komitmen. Dalam versi 2.0. x dan yang lebih baru, memanggil fungsi ini adalah opsional dan dibutuhkan semua nilai yang valid. Kebijakan komitmen default untuk versi 2.0. x dan yang lebih `COMMITMENT_POLICY_REQUIRE_ENCRYPT_REQUIRE_DECRYPT` baru

Untuk contoh lengkap, lihat string.cpp.

```
/* Load error strings for debugging */
aws_cryptosdk_load_error_strings();

/* Create an AWS KMS keyring */
const char * key_arn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
struct aws_cryptosdk_keyring *kms_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn);

/* Create an encrypt session with a CommitmentPolicy setting */
struct aws_cryptosdk_session *encrypt_session =
 aws_cryptosdk_session_new_from_keyring_2(
    alloc, AWS_CRYPTOSDK_ENCRYPT, kms_keyring);

aws_cryptosdk_keyring_release(kms_keyring);
aws_cryptosdk_session_set_commitment_policy(encrypt_session,
    COMMITMENT_POLICY_FORBID_ENCRYPT_ALLOW_DECRYPT);

...
/* Encrypt your data */

size_t plaintext_consumed_output;
aws_cryptosdk_session_process(encrypt_session,
```

```
                                ciphertext_output,
                                ciphertext_buf_sz_output,
                                ciphertext_len_output,
                                plaintext_input,
                                plaintext_len_input,
                                &plaintext_consumed_output)
...

/* Create a decrypt session with a CommitmentPolicy setting */

struct aws_cryptosdk_keyring *kms_keyring =
 Aws::Cryptosdk::KmsKeyring::Builder().Build(key_arn);
struct aws_cryptosdk_session *decrypt_session =
 *aws_cryptosdk_session_new_from_keyring_2(
        alloc, AWS_CRYPTOSDK_DECRYPT, kms_keyring);
aws_cryptosdk_keyring_release(kms_keyring);
aws_cryptosdk_session_set_commitment_policy(decrypt_session,
        COMMITMENT_POLICY_FORBID_ENCRYPT_ALLOW_DECRYPT);

/* Decrypt your ciphertext */
size_t ciphertext_consumed_output;
aws_cryptosdk_session_process(decrypt_session,
                                plaintext_output,
                                plaintext_buf_sz_output,
                                plaintext_len_output,
                                ciphertext_input,
                                ciphertext_len_input,
                                &ciphertext_consumed_output)
```

C# / .NET

`require-encrypt-require-decrypt`Nilai adalah kebijakan komitmen default di semua versi AWS Encryption SDK untuk .NET. Anda dapat mengaturnya secara eksplisit sebagai praktik terbaik, tetapi itu tidak diperlukan. Namun, jika Anda menggunakan AWS Encryption SDK untuk.NET untuk mendekripsi ciphertext yang dienkripsi oleh implementasi bahasa lain dari komitmen AWS Encryption SDK tanpa kunci, Anda perlu mengubah nilai kebijakan komitmen menjadi atau. `REQUIRE_ENCRYPT_ALLOW_DECRYPT` `FORBID_ENCRYPT_ALLOW_DECRYPT` Jika tidak, upaya untuk mendekripsi ciphertext akan gagal.

Dalam AWS Encryption SDK untuk .NET, Anda menetapkan kebijakan komitmen pada instance AWS Encryption SDK. Buat instance `AwsEncryptionSdkConfig` objek dengan `CommitmentPolicy` parameter, dan gunakan objek konfigurasi untuk membuat instance. AWS

Encryption SDK Kemudian, panggil `Encrypt()` dan `Decrypt()` metode dari AWS Encryption SDK instance yang dikonfigurasi.

Contoh ini menetapkan kebijakan komitmen untuk`require-encrypt-allow-decrypt`.

```
// Instantiate the material providers
var materialProviders =

 AwsCryptographicMaterialProvidersFactory.CreateDefaultAwsCryptographicMaterialProviders();

// Configure the commitment policy on the AWS Encryption SDK instance
var config = new AwsEncryptionSdkConfig
{
    CommitmentPolicy = CommitmentPolicy.REQUIRE_ENCRYPT_ALLOW_DECRYPT
};
var encryptionSdk = AwsEncryptionSdkFactory.CreateAwsEncryptionSdk(config);

string keyArn = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

var encryptionContext = new Dictionary<string, string>()
{
    {"purpose", "test"}encryptionSdk
};

var createKeyringInput = new CreateAwsKmsKeyringInput
{
    KmsClient = new AmazonKeyManagementServiceClient(),
    KmsKeyId = keyArn
};
var keyring = materialProviders.CreateAwsKmsKeyring(createKeyringInput);

// Encrypt your plaintext data
var encryptInput = new EncryptInput
{
    Plaintext = plaintext,
    Keyring = keyring,
    EncryptionContext = encryptionContext
};
var encryptOutput = encryptionSdk.Encrypt(encryptInput);

// Decrypt your ciphertext
var decryptInput = new DecryptInput
{
```

```
    Ciphertext = ciphertext,
    Keyring = keyring
};
var decryptOutput = encryptionSdk.Decrypt(decryptInput);
```

AWS Encryption CLI

Untuk menetapkan kebijakan komitmen dalam CLI AWS Enkripsi, gunakan parameter. `--commitment-policy` Parameter ini diperkenalkan dalam versi 1.8. x.

Yang terbaru 1. versi x, ketika Anda menggunakan `--wrapping-keys` parameter dalam `--decrypt` perintah `--encrypt` atau, `--commitment-policy` parameter dengan `forbid-encrypt-allow-decrypt` nilai diperlukan. Jika tidak, `--commitment-policy` parameternya tidak valid.

Dalam versi 2.1. x dan yang lebih baru, `--commitment-policy` parameternya opsional dan default ke `require-encrypt-require-decrypt` nilai, yang tidak akan mengenkripsi atau mendekripsi ciphertext apa pun yang dienkripsi tanpa komitmen kunci. Namun, kami menyarankan agar Anda menetapkan kebijakan komitmen secara eksplisit di semua panggilan enkripsi dan dekripsi untuk membantu pemeliharaan dan pemecahan masalah.

Contoh ini menetapkan kebijakan komitmen. Ini juga menggunakan `--wrapping-keys` parameter yang menggantikan `--master-keys` parameter yang dimulai pada versi 1.8. x. Lihat perinciannya di the section called “Memperbarui penyedia kunci AWS KMS utama”. Untuk contoh lengkap, lihatContoh CLI AWS Enkripsi.

```
\\ To run this example, replace the fictitious key ARN with a valid value.
$ keyArn=arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

\\ Encrypt your plaintext data - no change to algorithm suite used
$ aws-encryption-cli --encrypt \
                     --input hello.txt \
                     --wrapping-keys key=$keyArn \
                     --commitment-policy forbid-encrypt-allow-decrypt \
                     --metadata-output ~/metadata \
                     --encryption-context purpose=test \
                     --output .

\\ Decrypt your ciphertext - supports key commitment on 1.7 and later
$ aws-encryption-cli --decrypt \
                     --input hello.txt.encrypted \
                     --wrapping-keys key=$keyArn \
```

```
                    --commitment-policy forbid-encrypt-allow-decrypt \
                    --encryption-context purpose=test \
                    --metadata-output ~/metadata \
                    --output .
```

Java

Dimulai pada versi 1.7. x dari AWS Encryption SDK for Java, Anda menetapkan kebijakan komitmen pada instance Anda`AwsCrypto`, objek yang mewakili AWS Encryption SDK klien. Pengaturan kebijakan komitmen ini berlaku untuk semua operasi enkripsi dan dekripsi yang dipanggil pada klien tersebut.

`AwsCrypto()`Konstruktor tidak digunakan lagi di 1 terbaru. x versi AWS Encryption SDK for Java dan dihapus dalam versi 2.0. x. Ini digantikan oleh `Builder` kelas baru, `Builder.withCommitmentPolicy()` metode, dan tipe `CommitmentPolicy` enumerasi.

Yang terbaru 1. x versi, `Builder` kelas membutuhkan `Builder.withCommitmentPolicy()` metode dan `CommitmentPolicy.ForbidEncryptAllowDecrypt` argumen. Dimulai pada versi 2.0. x, `Builder.withCommitmentPolicy()` metode ini opsional; nilai defaultnya adalah`CommitmentPolicy.RequireEncryptRequireDecrypt`.

Untuk contoh lengkap, lihat SetCommitmentPolicyExample.java.

```
// Instantiate the client
final AwsCrypto crypto = AwsCrypto.builder()
    .withCommitmentPolicy(CommitmentPolicy.ForbidEncryptAllowDecrypt)
    .build();

// Create a master key provider in strict mode
String awsKmsKey = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

KmsMasterKeyProvider masterKeyProvider = KmsMasterKeyProvider.builder()
    .buildStrict(awsKmsKey);

// Encrypt your plaintext data
CryptoResult<byte[], KmsMasterKey> encryptResult = crypto.encryptData(
    masterKeyProvider,
    sourcePlaintext,
    encryptionContext);
byte[] ciphertext = encryptResult.getResult();
```

```
// Decrypt your ciphertext
CryptoResult<byte[], KmsMasterKey> decryptResult = crypto.decryptData(
        masterKeyProvider,
        ciphertext);
byte[] decrypted = decryptResult.getResult();
```

JavaScript

Dimulai pada versi 1.7. x dari AWS Encryption SDK for JavaScript, Anda dapat mengatur kebijakan komitmen ketika Anda memanggil `buildClient` fungsi baru yang membuat instance AWS Encryption SDK klien. `buildClient`Fungsi ini mengambil nilai yang disebutkan yang mewakili kebijakan komitmen Anda. Ini mengembalikan `decrypt` fungsi yang diperbarui `encrypt` dan yang menegakkan kebijakan komitmen Anda saat Anda mengenkripsi dan mendekripsi.

Yang terbaru 1. x versi, `buildClient` fungsi membutuhkan `CommitmentPolicy.FORBID_ENCRYPT_ALLOW_DECRYPT` argumen. Dimulai pada versi 2.0. x, argumen kebijakan komitmen adalah opsional dan nilai defaultnya adalah`CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT`.

Kode untuk Node.js dan browser identik untuk tujuan ini, kecuali bahwa browser membutuhkan pernyataan untuk mengatur kredensialnya.

Contoh berikut mengenkripsi data dengan keyring. AWS KMS `buildClient`Fungsi baru menetapkan kebijakan komitmen ke`FORBID_ENCRYPT_ALLOW_DECRYPT`, nilai default di 1 terbaru. x versin. Upgrade `encrypt` dan `decrypt` fungsi yang `buildClient` dikembalikan menegakkan kebijakan komitmen yang Anda tetapkan.

```
import { buildClient } from '@aws-crypto/client-node'
const { encrypt, decrypt } =
 buildClient(CommitmentPolicy.FORBID_ENCRYPT_ALLOW_DECRYPT)

// Create an AWS KMS keyring
const generatorKeyId = 'arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias'
const keyIds = ['arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab']
const keyring = new KmsKeyringNode({ generatorKeyId, keyIds })

// Encrypt your plaintext data
const { ciphertext } = await encrypt(keyring, plaintext, { encryptionContext:
 context })
```

```
// Decrypt your ciphertext
const { decrypted, messageHeader } = await decrypt(keyring, ciphertext)
```

Python

Dimulai pada versi 1.7. x dari AWS Encryption SDK for Python, Anda menetapkan kebijakan komitmen pada instance Anda`EncryptionSDKClient`, objek baru yang mewakili AWS Encryption SDK klien. Kebijakan komitmen yang Anda tetapkan berlaku untuk semua `encrypt` dan `decrypt` panggilan yang menggunakan instance klien tersebut.

Yang terbaru 1. x versi, `EncryptionSDKClient` konstruktor membutuhkan nilai yang `CommitmentPolicy.FORBID_ENCRYPT_ALLOW_DECRYPT` disebutkan. Dimulai pada versi 2.0. x, argumen kebijakan komitmen adalah opsional dan nilai defaultnya adalah`CommitmentPolicy.REQUIRE_ENCRYPT_REQUIRE_DECRYPT`.

Contoh ini menggunakan `EncryptionSDKClient` konstruktor baru dan menetapkan kebijakan komitmen ke 1.7. x nilai default. Konstruktor membuat instance klien yang mewakili. AWS Encryption SDK Ketika Anda memanggil`encrypt`,`decrypt`, atau `stream` metode pada klien ini, mereka menegakkan kebijakan komitmen yang Anda tetapkan. Contoh ini juga menggunakan konstruktor baru untuk `StrictAwsKmsMasterKeyProvider` kelas, yang menentukan AWS KMS keys saat mengenkripsi dan mendekripsi.

Untuk contoh lengkap, lihat set_commitment.py.

```
# Instantiate the client
client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.FORBID_ENCRYPT_AL

// Create a master key provider in strict mode
aws_kms_key = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
aws_kms_strict_master_key_provider = StrictAwsKmsMasterKeyProvider(
        key_ids=[aws_kms_key]
)

# Encrypt your plaintext data
ciphertext, encrypt_header = client.encrypt(
        source=source_plaintext,
        encryption_context=encryption_context,
        master_key_provider=aws_kms_strict_master_key_provider
```

```
)

# Decrypt your ciphertext
decrypted, decrypt_header = client.decrypt(
        source=ciphertext,
        master_key_provider=aws_kms_strict_master_key_provider
)
```

Rust

`require-encrypt-require-decrypt`Nilainya adalah kebijakan komitmen default di semua versi AWS Encryption SDK untuk Rust. Anda dapat mengaturnya secara eksplisit sebagai praktik terbaik, tetapi itu tidak diperlukan. Namun, jika Anda menggunakan AWS Encryption SDK for Rust untuk mendekripsi ciphertext yang dienkripsi oleh implementasi bahasa lain dari komitmen AWS Encryption SDK tanpa kunci, Anda perlu mengubah nilai kebijakan komitmen menjadi atau. `REQUIRE_ENCRYPT_ALLOW_DECRYPT` `FORBID_ENCRYPT_ALLOW_DECRYPT` Jika tidak, upaya untuk mendekripsi ciphertext akan gagal.

Dalam AWS Encryption SDK for Rust, Anda menetapkan kebijakan komitmen pada instance AWS Encryption SDK. Buat instance `AwsEncryptionSdkConfig` objek dengan `comitment_policy` parameter, dan gunakan objek konfigurasi untuk membuat instance. AWS Encryption SDK Kemudian, panggil `Encrypt()` dan `Decrypt()` metode dari AWS Encryption SDK instance yang dikonfigurasi.

Contoh ini menetapkan kebijakan komitmen untuk`forbid-encrypt-allow-decrypt`.

```
// Configure the commitment policy on the AWS Encryption SDK instance
let esdk_config = AwsEncryptionSdkConfig::builder()
                    .commitment_policy(ForbidEncryptAllowDecrypt)
                    .build()?;
let esdk_client = esdk_client::Client::from_conf(esdk_config)?;

// Create an AWS KMS client
let sdk_config =
 aws_config::load_defaults(aws_config::BehaviorVersion::latest()).await;
let kms_client = aws_sdk_kms::Client::new(&sdk_config);

// Create your encryption context
let encryption_context = HashMap::from([
    ("encryption".to_string(), "context".to_string()),
    ("is not".to_string(), "secret".to_string()),
    ("but adds".to_string(), "useful metadata".to_string()),
```

```
    ("that can help you".to_string(), "be confident that".to_string()),
    ("the data you are handling".to_string(), "is what you think it
 is".to_string()),
]);

// Instantiate the material providers library
let mpl_config = MaterialProvidersConfig::builder().build()?;
let mpl = mpl_client::Client::from_conf(mpl_config)?;

// Create an AWS KMS keyring
let kms_keyring = mpl
    .create_aws_kms_keyring()
    .kms_key_id(kms_key_id)
    .kms_client(kms_client)
    .send()
    .await?;

// Encrypt your plaintext data
let plaintext = example_data.as_bytes();

let encryption_response = esdk_client.encrypt()
    .plaintext(plaintext)
    .keyring(kms_keyring.clone())
    .encryption_context(encryption_context.clone())
    .send()
    .await?;

// Decrypt your ciphertext
let decryption_response = esdk_client.decrypt()
    .ciphertext(ciphertext)
    .keyring(kms_keyring)
    // Provide the encryption context that was supplied to the encrypt method
    .encryption_context(encryption_context)
    .send()
    .await?;
```

Go

```
import (
    "context"

 mpl "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygenerated"
```

```
 mpltypes "aws/aws-cryptographic-material-providers-library/releases/go/mpl/
awscryptographymaterialproviderssmithygeneratedtypes"
 client "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygenerated"
 esdktypes "github.com/aws/aws-encryption-sdk/
awscryptographyencryptionsdksmithygeneratedtypes"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/kms"
)

// Instantiate the AWS Encryption SDK client
commitPolicyForbidEncryptAllowDecrypt :=
 mpltypes.ESDKCommitmentPolicyForbidEncryptAllowDecrypt
encryptionClient, err :=
 client.NewClient(esdktypes.AwsEncryptionSdkConfig{CommitmentPolicy:
 &commitPolicyForbidEncryptAllowDecrypt})
if err != nil {
    panic(err)
}

// Create an AWS KMS client
cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic(err)
}
kmsClient := kms.NewFromConfig(cfg, func(o *kms.Options) {
    o.Region = KmsKeyRegion
})

// Optional: Create an encryption context
encryptionContext := map[string]string{
    "encryption":               "context",
    "is not":                   "secret",
    "but adds":                 "useful metadata",
    "that can help you":        "be confident that",
    "the data you are handling": "is what you think it is",
}

// Instantiate the material providers library
matProv, err := mpl.NewClient(mpltypes.MaterialProvidersConfig{})
if err != nil {
    panic(err)
}
```

```
// Create an AWS KMS keyring
awsKmsKeyringInput := mpltypes.CreateAwsKmsKeyringInput{
    KmsClient: kmsClient,
    KmsKeyId:  kmsKeyId,
}
awsKmsKeyring, err := matProv.CreateAwsKmsKeyring(context.Background(),
 awsKmsKeyringInput)
if err != nil {
    panic(err)
}

// Encrypt your plaintext data
res, err := forbidEncryptClient.Encrypt(context.Background(),
 esdktypes.EncryptInput{
    Plaintext:         []byte(exampleText),
    EncryptionContext: encryptionContext,
    Keyring:           awsKmsKeyring,
})
if err != nil {
    panic(err)
}

// Decrypt your ciphertext
decryptOutput, err := forbidEncryptClient.Decrypt(context.Background(),
 esdktypes.DecryptInput{
    Ciphertext:        res.Ciphertext,
    EncryptionContext: encryptionContext,
    Keyring:           awsKmsKeyring,
})
if err != nil {
    panic(err)
}
```

Memecahkan masalah migrasi ke versi terbaru

Sebelum memperbarui aplikasi Anda ke versi 2.0. x atau yang lebih baru AWS Encryption SDK, perbarui ke yang terbaru 1. x versi AWS Encryption SDK dan terapkan sepenuhnya. Itu akan membantu Anda menghindari sebagian besar kesalahan yang mungkin Anda temui saat memperbarui ke versi 2.0. x dan kemudian. Untuk panduan terperinci, termasuk contoh, lihatMigrasi Anda AWS Encryption SDK.

> **Important**
>
> Verifikasi bahwa terbaru Anda 1. Versi x adalah versi 1.7. x atau yang lebih baru AWS Encryption SDK.

> **Note**
>
> AWS Enkripsi CLI: Referensi dalam panduan ini ke versi 1.7. x AWS Encryption SDK berlaku untuk versi 1.8. x dari CLI AWS Enkripsi. Referensi dalam panduan ini ke versi 2.0. x dari AWS Encryption SDK berlaku untuk 2.1. x dari CLI AWS Enkripsi.
> Fitur keamanan baru awalnya dirilis dalam AWS Enkripsi CLI versi 1.7. x dan 2.0. x. Namun, AWS Enkripsi CLI versi 1.8. x menggantikan versi 1.7. x dan AWS Enkripsi CLI 2.1. x menggantikan 2.0. x. Untuk detailnya, lihat penasihat keamanan yang relevan di aws-encryption-sdk-clirepositori di. GitHub

Topik ini dirancang untuk membantu Anda mengenali dan mengatasi kesalahan paling umum yang mungkin Anda temui.

Topik

Objek yang tidak digunakan lagi atau dihapus

Versi 2.0. x mencakup beberapa perubahan yang melanggar, termasuk menghapus konstruktor lama, metode, fungsi, dan kelas yang tidak digunakan lagi di versi 1.7. x. Untuk menghindari kesalahan kompiler, kesalahan impor, kesalahan sintaks, dan kesalahan simbol tidak ditemukan (tergantung pada bahasa pemrograman Anda), tingkatkan terlebih dahulu ke yang terbaru 1. x versi

AWS Encryption SDK untuk bahasa pemrograman Anda. (Ini harus versi 1.7. x atau yang lebih baru.) Saat menggunakan yang terbaru 1. x versi, Anda dapat mulai menggunakan elemen pengganti sebelum simbol asli dihapus.

Jika Anda perlu meng-upgrade ke versi 2.0. x atau yang lebih baru segera, konsultasikan changelog untuk bahasa pemrograman Anda, dan ganti simbol warisan dengan simbol yang direkomendasikan changelog.

Konflik konfigurasi: Kebijakan komitmen dan rangkaian algoritme

Jika Anda menentukan rangkaian algoritme yang bertentangan dengan kebijakan komitmen Anda, panggilan untuk mengenkripsi gagal dengan kesalahan konflik Konfigurasi.

Untuk menghindari jenis kesalahan ini, jangan tentukan rangkaian algoritme. Secara default, AWS Encryption SDK memilih algoritma paling aman yang kompatibel dengan kebijakan komitmen Anda. Namun, jika Anda harus menentukan rangkaian algoritme, seperti tanpa penandatanganan, pastikan untuk memilih rangkaian algoritme yang kompatibel dengan kebijakan komitmen Anda.

Kebijakan komitmen	Suite algoritma yang kompatibel
ForbidEncryptAllowDecrypt	Setiap rangkaian algoritma tanpa komitmen utama, seperti: `AES_256_GCM_IV12_TAG16_HKDF_SHA384_ECDSA_P384` (03 78) (dengan penandatanganan) `AES_256_GCM_IV12_TAG16_HKDF_SHA256` (01 78) (tanpa penandatanganan)
RequireEncryptAllowDecrypt RequireEncryptRequireDecrypt	Setiap rangkaian algoritma dengan komitmen utama, seperti: `AES_256_GCM_HKDF_SHA512_COMMIT_KEY_ECDSA_P384` (05 78) (dengan penandatanganan) `AES_256_GCM_HKDF_SHA512_COMMIT_KEY` (04 78) (tanpa penandatanganan)

Jika Anda mengalami kesalahan ini ketika Anda belum menentukan rangkaian algoritme, rangkaian algoritme yang bertentangan mungkin telah dipilih oleh pengelola bahan kriptografi (CMM) Anda. CMM Default tidak akan memilih rangkaian algoritme yang bertentangan, tetapi CMM khusus mungkin. Untuk bantuan, lihat dokumentasi untuk CMM kustom Anda.

Konflik konfigurasi: Kebijakan komitmen dan ciphertext

Kebijakan `RequireEncryptRequireDecrypt` komitmen tidak mengizinkan AWS Encryption SDK untuk mendekripsi pesan yang dienkripsi tanpa komitmen utama. Jika Anda meminta AWS Encryption SDK untuk mendekripsi pesan tanpa komitmen kunci, ia mengembalikan kesalahan konflik Konfigurasi.

Untuk menghindari kesalahan ini, sebelum menetapkan kebijakan `RequireEncryptRequireDecrypt` komitmen, pastikan bahwa semua ciphertext yang dienkripsi tanpa komitmen utama didekripsi dan dienkripsi ulang dengan komitmen utama, atau ditangani oleh aplikasi yang berbeda. Jika Anda mengalami kesalahan ini, Anda dapat mengembalikan kesalahan untuk ciphertext yang bertentangan atau mengubah kebijakan komitmen Anda untuk sementara. `RequireEncryptAllowDecrypt`

Jika Anda mengalami kesalahan ini karena Anda meningkatkan ke versi 2.0. x atau lebih baru dari versi lebih awal dari 1.7. x tanpa upgrade terlebih dahulu ke yang terbaru 1. x versi (versi 1.7. x atau lebih baru), pertimbangkan untuk memutar kembali ke yang terbaru 1. x versi dan menyebarkan versi itu ke semua host sebelum memutakhirkan ke versi 2.0. x atau yang lebih baru. Untuk bantuan, lihat Cara memigrasi dan menyebarkan AWS Encryption SDK.

Validasi komitmen utama gagal

Saat mendekripsi pesan yang dienkripsi dengan komitmen utama, Anda mungkin mendapatkan pesan galat gagal validasi komitmen Kunci. Ini menunjukkan bahwa panggilan dekripsi gagal karena kunci data dalam pesan terenkripsi tidak identik dengan kunci data unik untuk pesan tersebut. Dengan memvalidasi kunci data selama dekripsi, komitmen kunci melindungi Anda dari mendekripsi pesan yang mungkin menghasilkan lebih dari satu teks biasa.

Kesalahan ini menunjukkan bahwa pesan terenkripsi yang Anda coba dekripsi tidak dikembalikan oleh. AWS Encryption SDK Ini mungkin pesan yang dibuat secara manual atau hasil dari korupsi data. Jika Anda mengalami kesalahan ini, aplikasi Anda dapat menolak pesan dan melanjutkan, atau berhenti memproses pesan baru.

Kegagalan enkripsi lainnya

Enkripsi dapat gagal karena berbagai alasan. Anda tidak dapat menggunakan keyring AWS KMS penemuan atau penyedia kunci utama dalam mode penemuan untuk mengenkripsi pesan.

Pastikan Anda menentukan keyring atau penyedia kunci master dengan kunci pembungkus yang memiliki izin untuk digunakan untuk enkripsi. Untuk bantuan terkait izin AWS KMS keys, lihat Melihat kebijakan utama dan Menentukan akses ke AWS KMS key dalam Panduan AWS Key Management Service Pengembang.

Kegagalan dekripsi lainnya

Jika upaya Anda untuk mendekripsi pesan terenkripsi gagal, itu berarti bahwa tidak AWS Encryption SDK dapat (atau tidak akan) mendekripsi salah satu kunci data terenkripsi dalam pesan.

Jika Anda menggunakan keyring atau penyedia kunci master yang menentukan kunci pembungkus, hanya AWS Encryption SDK menggunakan kunci pembungkus yang Anda tentukan. Verifikasi bahwa Anda menggunakan kunci pembungkus yang Anda inginkan dan bahwa Anda memiliki `kms:Decrypt` izin pada setidaknya satu dari kunci pembungkus. Jika Anda menggunakan AWS KMS keys, sebagai fallback, Anda dapat mencoba mendekripsi pesan dengan keyring AWS KMS penemuan atau penyedia kunci utama dalam mode penemuan. Jika operasi berhasil, sebelum mengembalikan plaintext, verifikasi bahwa kunci yang digunakan untuk mendekripsi pesan adalah kunci yang Anda percayai.

Pertimbangan rollback

Jika aplikasi Anda gagal mengenkripsi atau mendekripsi data, Anda biasanya dapat menyelesaikan masalah dengan memperbarui simbol kode, keyrings, penyedia kunci master, atau kebijakan komitmen. Namun, dalam beberapa kasus, Anda mungkin memutuskan bahwa yang terbaik adalah memutar kembali aplikasi Anda ke versi sebelumnya AWS Encryption SDK.

Jika Anda harus memutar kembali, lakukan dengan hati-hati. Versi AWS Encryption SDK sebelum 1.7. x tidak dapat mendekripsi ciphertext yang dienkripsi dengan komitmen utama.

- Bergulir kembali dari yang terbaru 1. versi x ke versi sebelumnya AWS Encryption SDK umumnya aman. Anda mungkin harus membatalkan perubahan yang Anda buat pada kode Anda untuk menggunakan simbol dan objek yang tidak didukung di versi sebelumnya.
- Setelah Anda mulai mengenkripsi dengan komitmen utama (menetapkan kebijakan komitmen Anda`RequireEncryptAllowDecrypt`) di versi 2.0. x atau yang lebih baru, Anda dapat memutar

kembali ke versi 1.7. x, tetapi tidak ke versi sebelumnya. Versi AWS Encryption SDK sebelum 1.7. x tidak dapat mendekripsi ciphertext yang dienkripsi dengan komitmen utama.

Jika Anda secara tidak sengaja mengaktifkan enkripsi dengan komitmen utama sebelum semua host dapat mendekripsi dengan komitmen utama, mungkin yang terbaik adalah melanjutkan peluncuran daripada memutar kembali. Jika pesan bersifat sementara atau dapat dijatuhkan dengan aman, maka Anda dapat mempertimbangkan rollback dengan hilangnya pesan. Jika rollback diperlukan, Anda dapat mempertimbangkan untuk menulis alat yang mendekripsi dan mengenkripsi ulang semua pesan.

Pertanyaan umum

Pertanyaan umum

Bagaimana AWS Encryption SDK bedanya dengan AWS SDKs?

Ini AWS SDKsmenyediakan pustaka untuk berinteraksi dengan Amazon Web Services (AWS), termasuk AWS Key Management Service (AWS KMS). Beberapa implementasi bahasa AWS Encryption SDK, seperti AWS Encryption SDK untuk .NET, selalu memerlukan AWS SDK dalam bahasa pemrograman yang sama. Implementasi bahasa lain memerlukan AWS SDK yang sesuai hanya jika Anda menggunakan AWS KMS kunci di keyrings atau penyedia kunci utama. Untuk detailnya, lihat topik tentang bahasa pemrograman Anda diAWS Encryption SDK bahasa pemrograman.

Anda dapat menggunakan file AWS SDKs untuk berinteraksi AWS KMS, termasuk mengenkripsi dan mendekripsi sejumlah kecil data (hingga 4.096 byte dengan kunci enkripsi simetris) dan menghasilkan kunci data untuk enkripsi sisi klien. Namun, ketika Anda membuat kunci data, Anda

harus mengelola seluruh proses enkripsi dan dekripsi, termasuk mengenkripsi data Anda dengan kunci data di luar, membuang kunci data teks biasa dengan aman AWS KMS, menyimpan kunci data terenkripsi, dan kemudian mendekripsi kunci data dan mendekripsi data Anda. AWS Encryption SDK Menangani proses ini untuk Anda.

AWS Encryption SDK Ini menyediakan perpustakaan yang mengenkripsi dan mendekripsi data menggunakan standar industri dan praktik terbaik. Ini menghasilkan kunci data, mengenkripsi di bawah kunci pembungkus yang Anda tentukan, dan mengembalikan pesan terenkripsi, objek data portabel yang mencakup data terenkripsi dan kunci data terenkripsi yang Anda butuhkan untuk mendekripsi itu. Ketika tiba waktunya untuk mendekripsi, Anda meneruskan pesan terenkripsi dan setidaknya salah satu kunci pembungkus (opsional), dan mengembalikan data plaintext Anda. AWS Encryption SDK

Anda dapat menggunakan AWS KMS keys sebagai kunci pembungkus di AWS Encryption SDK, tetapi tidak diperlukan. Anda dapat menggunakan kunci enkripsi yang Anda buat dan kunci dari pengelola kunci atau modul keamanan perangkat keras lokal. Anda dapat menggunakan AWS Encryption SDK bahkan jika Anda tidak memiliki AWS akun.

Apa AWS Encryption SDK bedanya dengan klien enkripsi Amazon S3?

Klien enkripsi Amazon S3 di dalamnya AWS SDKs menyediakan enkripsi dan dekripsi untuk data yang Anda simpan di Amazon Simple Storage Service (Amazon S3). Klien ini digabungkan erat ke Amazon S3 dan dimaksudkan untuk digunakan hanya dengan data yang disimpan di sana.

AWS Encryption SDK Ini menyediakan enkripsi dan dekripsi untuk data yang dapat Anda simpan di mana saja. Klien enkripsi Amazon S3 AWS Encryption SDK dan Amazon S3 tidak kompatibel karena mereka menghasilkan ciphertext dengan format data yang berbeda.

Algoritma kriptografi mana yang didukung oleh AWS Encryption SDK, dan mana yang merupakan default?

AWS Encryption SDK Menggunakan algoritma simetris Advanced Encryption Standard (AES) dalam Galois/Counter Mode (GCM), yang dikenal sebagai AES-GCM, untuk mengenkripsi data Anda. Ini memungkinkan Anda memilih dari beberapa algoritma simetris dan asimetris untuk mengenkripsi kunci data yang mengenkripsi data Anda.

Untuk AES-GCM, rangkaian algoritme default adalah AES-GCM dengan kunci 256-bit, derivasi kunci (HKDF), tanda tangan digital, dan komitmen kunci. AWS Encryption SDK juga mendukung kunci enkripsi 192-bit, dan 128-bit dan algoritma enkripsi tanpa tanda tangan digital dan komitmen utama.

Dalam semua kasus, panjang vektor inisialisasi (IV) adalah 12 byte; panjang tag otentikasi adalah 16 byte. Secara default, SDK menggunakan kunci data sebagai input ke fungsi derivasi kunci berbasis HMAC (HKDF) untuk mendapatkan extract-and-expand kunci enkripsi AES-GCM, dan juga menambahkan tanda tangan Elliptic Curve Digital Signature Algorithm (ECDSA).

Untuk informasi tentang memilih algoritma mana yang akan digunakan, lihatSuite algoritma yang didukung.

Untuk detail implementasi tentang algoritme yang didukung, lihatReferensi algoritma.

Bagaimana vektor inisialisasi (IV) dihasilkan dan di mana disimpan?

AWS Encryption SDK Menggunakan metode deterministik untuk membangun nilai IV yang berbeda untuk setiap frame. Prosedur ini menjamin bahwa tidak pernah IVs diulang dalam pesan. (Sebelum versi 1.3.0 AWS Encryption SDK for Java dan AWS Encryption SDK for Python, nilai IV unik yang dihasilkan AWS Encryption SDK secara acak untuk setiap frame.)

IV disimpan dalam pesan terenkripsi yang dikembalikan. AWS Encryption SDK Untuk informasi selengkapnya, lihat AWS Encryption SDK referensi format pesan.

Bagaimana setiap kunci data dihasilkan, dienkripsi, dan didekripsi?

Metode ini tergantung pada keyring atau penyedia kunci master yang Anda gunakan.

AWS KMS Keyrings dan penyedia kunci master dalam AWS Encryption SDK menggunakan operasi AWS KMS GenerateDataKeyAPI untuk menghasilkan setiap kunci data dan mengenkripsinya di bawah kunci pembungkusnya. Untuk mengenkripsi salinan kunci data di bawah kunci KMS tambahan, mereka menggunakan operasi AWS KMS Enkripsi. Untuk mendekripsi kunci data, mereka menggunakan operasi AWS KMS Dekripsi. Untuk detailnya, lihat AWS KMS keyring di AWS Encryption SDK Spesifikasi di GitHub.

Keyring lain menghasilkan kunci data, mengenkripsi, dan mendekripsi menggunakan metode praktik terbaik untuk setiap bahasa pemrograman. Untuk detailnya, lihat spesifikasi keyring atau penyedia kunci utama di bagian Kerangka AWS Encryption SDK Spesifikasi di GitHub.

Bagaimana cara melacak kunci data yang digunakan untuk mengenkripsi data saya?

Yang AWS Encryption SDK melakukan ini untuk Anda. Saat Anda mengenkripsi data, SDK mengenkripsi kunci data dan menyimpan kunci terenkripsi bersama dengan data terenkripsi dalam pesan terenkripsi yang dikembalikan. Ketika Anda mendekripsi data, AWS Encryption SDK mengekstrak kunci data terenkripsi dari pesan terenkripsi, mendekripsi, dan kemudian menggunakannya untuk mendekripsi data.

Bagaimana cara AWS Encryption SDK menyimpan kunci data terenkripsi dengan data terenkripsi mereka?

Operasi enkripsi dalam AWS Encryption SDK mengembalikan pesan terenkripsi, struktur data tunggal yang berisi data terenkripsi dan kunci data terenkripsi. Format pesan terdiri dari setidaknya dua bagian: header dan badan. Header pesan berisi kunci data terenkripsi dan informasi tentang bagaimana badan pesan terbentuk. Badan pesan berisi data terenkripsi. Jika rangkaian algoritme menyertakan tanda tangan digital, format pesan menyertakan footer yang berisi tanda tangan. Untuk informasi selengkapnya, lihat AWS Encryption SDK referensi format pesan.

Berapa banyak overhead yang ditambahkan format AWS Encryption SDK pesan ke data terenkripsi saya?

Jumlah overhead yang ditambahkan oleh AWS Encryption SDK tergantung pada beberapa faktor, termasuk yang berikut:

- Ukuran data plaintext
- Manakah dari algoritma yang didukung yang digunakan
- Apakah data otentikasi tambahan (AAD) disediakan, dan panjang AAD itu
- Jumlah dan jenis kunci pembungkus atau kunci master
- Ukuran bingkai (saat data berbingkai digunakan)

Saat Anda menggunakan konfigurasi defaultnya (satu AWS KMS key sebagai kunci pembungkus (atau kunci master), tidak ada AAD, data tidak berbingkai, dan algoritme enkripsi dengan penandatanganan), overhead sekitar 600 byte. AWS Encryption SDK Secara umum, Anda dapat

berasumsi bahwa AWS Encryption SDK penambahan overhead 1 KB atau kurang, tidak termasuk AAD yang disediakan. Untuk informasi selengkapnya, lihat AWS Encryption SDK referensi format pesan.

Bisakah saya menggunakan penyedia kunci master saya sendiri?

Ya. Detail implementasi bervariasi tergantung pada bahasa pemrograman yang didukung yang Anda gunakan. Namun, semua bahasa yang didukung memungkinkan Anda untuk menentukan manajer materi kriptografi kustom (CMMs) Ms), penyedia kunci master, gantungan kunci, kunci master, dan kunci pembungkus.

Dapatkah saya mengenkripsi data di bawah lebih dari satu kunci pembungkus?

Ya. Anda dapat mengenkripsi kunci data dengan kunci pembungkus tambahan (atau kunci master) untuk menambahkan redundansi ketika kunci berada di wilayah yang berbeda atau tidak tersedia untuk dekripsi.

Untuk mengenkripsi data di bawah beberapa kunci pembungkus, buat keyring atau penyedia kunci master dengan beberapa kunci pembungkus. Saat bekerja dengan keyrings, Anda dapat membuat keyring tunggal dengan beberapa tombol pembungkus atau multi-keyring.

Saat Anda mengenkripsi data dengan beberapa kunci pembungkus, AWS Encryption SDK menggunakan satu kunci pembungkus untuk menghasilkan kunci data teks biasa. Kunci data unik dan secara matematis tidak terkait dengan kunci pembungkus. Operasi mengembalikan kunci data plaintext dan salinan kunci data yang dienkripsi oleh kunci pembungkus. Kemudian metode enkripsi, mengenkripsi kunci data dengan kunci pembungkus lainnya. Pesan terenkripsi yang dihasilkan mencakup data terenkripsi dan satu kunci data terenkripsi untuk setiap kunci pembungkus.

Pesan terenkripsi dapat didekripsi dengan menggunakan salah satu kunci pembungkus yang digunakan dalam operasi enkripsi. AWS Encryption SDK Menggunakan kunci pembungkus untuk mendekripsi kunci data terenkripsi. Kemudian, ia menggunakan kunci data plaintext untuk mendekripsi data.

Tipe data apa yang dapat saya enkripsi dengan? AWS Encryption SDK

Sebagian besar implementasi bahasa pemrograman AWS Encryption SDK dapat mengenkripsi byte mentah (byte array), I/O stream (byte stream), dan string. The AWS Encryption SDK for .NET tidak mendukung I/O aliran. Kami menyediakan contoh kode untuk masing-masing bahasa pemrograman yang didukung.

Bagaimana cara AWS Encryption SDK mengenkripsi dan mendekripsi input/output (I/O) mengalir?

AWS Encryption SDK Membuat aliran enkripsi atau dekripsi yang membungkus aliran yang mendasarinya. I/O Aliran enkripsi atau dekripsi melakukan operasi kriptografi pada panggilan baca atau tulis. Misalnya, ia dapat membaca data teks biasa pada aliran yang mendasarinya dan mengenkripsi sebelum mengembalikan hasilnya. Atau dapat membaca ciphertext dari aliran yang mendasarinya dan mendekripsi sebelum mengembalikan hasilnya. Kami menyediakan contoh kode untuk mengenkripsi dan mendekripsi aliran untuk setiap bahasa pemrograman yang didukung yang mendukung streaming.

The AWS Encryption SDK for .NET tidak mendukung I/O aliran.

AWS Encryption SDK referensi

Informasi di halaman ini adalah referensi untuk membangun pustaka enkripsi Anda sendiri yang kompatibel dengan file AWS Encryption SDK. Jika Anda tidak membangun pustaka enkripsi kompatibel Anda sendiri, Anda mungkin tidak memerlukan informasi ini.

Untuk menggunakan AWS Encryption SDK dalam salah satu bahasa pemrograman yang didukung, lihatBahasa pemrograman.

Untuk spesifikasi yang mendefinisikan elemen AWS Encryption SDK implementasi yang tepat, lihat AWS Encryption SDK Spesifikasi di GitHub.

AWS Encryption SDK Menggunakan algoritma yang didukung untuk mengembalikan struktur data tunggal atau pesan yang berisi data terenkripsi dan kunci data terenkripsi yang sesuai. Topik berikut menjelaskan algoritma dan struktur data. Gunakan informasi ini untuk membangun pustaka yang dapat membaca dan menulis ciphertext yang kompatibel dengan SDK ini.

Topik

- AWS Encryption SDK referensi format pesan
- AWS Encryption SDK contoh format pesan
- Referensi data terautentikasi tambahan badan (AAD) untuk AWS Encryption SDK
- AWS Encryption SDK referensi algoritma
- AWS Encryption SDK referensi vektor inisialisasi
- AWS KMS Rincian teknis keyring hierarkis

AWS Encryption SDK referensi format pesan

Informasi di halaman ini adalah referensi untuk membangun pustaka enkripsi Anda sendiri yang kompatibel dengan file AWS Encryption SDK. Jika Anda tidak membangun pustaka enkripsi kompatibel Anda sendiri, Anda mungkin tidak memerlukan informasi ini.

Untuk menggunakan AWS Encryption SDK dalam salah satu bahasa pemrograman yang didukung, lihatBahasa pemrograman.

Untuk spesifikasi yang mendefinisikan elemen AWS Encryption SDK implementasi yang tepat, lihat AWS Encryption SDK Spesifikasi di GitHub.

Operasi enkripsi dalam AWS Encryption SDK mengembalikan struktur data tunggal atau pesan terenkripsi yang berisi data terenkripsi (ciphertext) dan semua kunci data terenkripsi. Untuk memahami struktur data ini, atau untuk membangun pustaka yang membaca dan menulisnya, Anda perlu memahami format pesan.

Format pesan terdiri dari setidaknya dua bagian: header dan badan. Dalam beberapa kasus, format pesan terdiri dari bagian ketiga, footer. Format pesan mendefinisikan urutan urutan byte dalam urutan byte jaringan, juga disebut format big-endian. Format pesan dimulai dengan header, diikuti oleh tubuh, diikuti oleh footer (ketika ada).

Suite algoritma didukung oleh AWS Encryption SDK penggunaan salah satu dari dua versi format pesan. Suite algoritma tanpa komitmen utama menggunakan format pesan versi 1. Suite algoritma dengan komitmen utama menggunakan format pesan versi 2.

Topik

- Struktur header
- Struktur tubuh
- Struktur footer

Struktur header

Header pesan berisi kunci data terenkripsi dan informasi tentang bagaimana badan pesan terbentuk. Tabel berikut menjelaskan bidang yang membentuk header dalam format pesan versi 1 dan 2. Byte ditambahkan dalam urutan yang ditunjukkan.

Nilai tidak hadir menunjukkan bahwa bidang tidak ada dalam versi format pesan tersebut. Teks tebal menunjukkan nilai yang berbeda di setiap versi.

> **Note**
>
> Anda mungkin perlu menggulir secara horizontal atau vertikal untuk melihat semua data dalam tabel ini.

Struktur Header

Bidang	Format pesan versi 1 Panjang (byte)	Format pesan versi 2 Panjang (byte)
Version	1	1
Type	1	Tidak hadir
Algorithm ID	2	2
Message ID	16	32
AAD Length	2 Ketika konteks enkripsi kosong, nilai bidang Panjang AAD 2-byte adalah 0.	2 Ketika konteks enkripsi kosong, nilai bidang Panjang AAD 2-byte adalah 0.
AAD	Variabel. Panjang bidang ini muncul di 2 byte sebelumnya (bidang Panjang AAD). Ketika konteks enkripsi kosong, tidak ada bidang AAD di header.	Variabel. Panjang bidang ini muncul di 2 byte sebelumnya (bidang Panjang AAD). Ketika konteks enkripsi kosong, tidak ada bidang AAD di header.
Encrypted Data Key Count	2	2
Encrypted Data Key(s)	Variabel. Ditentukan oleh jumlah kunci data terenkripsi dan panjang masing-masing.	Variabel. Ditentukan oleh jumlah kunci data terenkripsi dan panjang masing-masing.
Content Type	1	1
Reserved	4	Tidak hadir
IV Length	1	Tidak hadir
Frame Length	4	4

Bidang	Format pesan versi 1 Panjang (byte)	Format pesan versi 2 Panjang (byte)
Algorithm Suite Data	Tidak hadir	Variabel. Ditentukan oleh algoritma yang menghasilkan pesan.
Header Authentication	Variabel. Ditentukan oleh algoritma yang menghasilkan pesan.	Variabel. Ditentukan oleh algoritma yang menghasilkan pesan.

Versi

Versi format pesan ini. Versi ini adalah 1 atau 2 dikodekan sebagai byte `01` atau `02` dalam notasi heksadesimal

Jenis

Jenis format pesan ini. Jenis menunjukkan jenis struktur. Satu-satunya jenis yang didukung digambarkan sebagai data terenkripsi yang diautentikasi pelanggan. Nilai tipenya adalah 128, dikodekan sebagai byte `80` dalam notasi heksadesimal.

Bidang ini tidak ada dalam format pesan versi 2.

ID Algoritma

Pengidentifikasi untuk algoritma yang digunakan. Ini adalah nilai 2-byte yang ditafsirkan sebagai integer unsigned 16-bit. Untuk informasi selengkapnya tentang algoritme, lihatAWS Encryption SDK referensi algoritma.

ID Pesan

Nilai yang dihasilkan secara acak yang mengidentifikasi pesan. ID Pesan:

- Mengidentifikasi pesan terenkripsi secara unik.
- Lemah mengikat header pesan ke badan pesan.
- Menyediakan mekanisme untuk menggunakan kembali kunci data dengan aman dengan beberapa pesan terenkripsi.
- Melindungi dari penggunaan kembali kunci data yang tidak disengaja atau keausan kunci di. AWS Encryption SDK

Nilai ini adalah 128 bit dalam format pesan versi 1 dan 256 bit dalam versi 2.

Panjang AAD

Panjang data otentikasi tambahan (AAD). Ini adalah nilai 2-byte ditafsirkan sebagai 16-bit unsigned integer yang menentukan jumlah byte yang berisi AAD.

Ketika konteks enkripsi kosong, nilai bidang Panjang AAD adalah 0.

AAD

Data tambahan yang diautentikasi. AAD adalah pengkodean konteks enkripsi, array pasangan kunci-nilai di mana setiap kunci dan nilai adalah string karakter yang dikodekan UTF-8. Konteks enkripsi dikonversi ke urutan byte dan digunakan untuk nilai AAD. Ketika konteks enkripsi kosong, tidak ada bidang AAD di header.

Ketika algoritma dengan penandatanganan digunakan, konteks enkripsi harus berisi pasangan kunci-nilai. `{'aws-crypto-public-key', Qtxt}` Qtxt mewakili titik kurva elips Q yang dikompresi menurut SEC 1 versi 2.0 dan kemudian dikodekan base64. Konteks enkripsi dapat berisi nilai tambahan, tetapi panjang maksimum AAD yang dibangun adalah 2 ^ 16 - 1 byte.

Tabel berikut menjelaskan bidang yang membentuk AAD. Pasangan nilai kunci diurutkan, berdasarkan kunci, dalam urutan menaik sesuai dengan kode karakter UTF-8. Byte ditambahkan dalam urutan yang ditunjukkan.

Struktur AAD

Bidang	Panjang (byte)
Key-Value Pair Count	2
Key Length	2
Key	Variabel. Sama dengan nilai yang ditentukan dalam 2 byte sebelumnya (Panjang Kunci).
Value Length	2
Value	Variabel. Sama dengan nilai yang ditentukan dalam 2 byte sebelumnya (Value Length).

Hitungan Pasangan Nilai Kunci

Jumlah pasangan kunci-nilai di AAD. Ini adalah nilai 2-byte yang ditafsirkan sebagai integer unsigned 16-bit yang menentukan jumlah pasangan kunci-nilai di AAD. Jumlah maksimum pasangan kunci-nilai dalam AAD adalah 2^16 - 1.

Ketika tidak ada konteks enkripsi atau konteks enkripsi kosong, bidang ini tidak ada dalam struktur AAD.

Panjang Kunci

Panjang kunci untuk pasangan kunci-nilai. Ini adalah nilai 2-byte ditafsirkan sebagai 16-bit unsigned integer yang menentukan jumlah byte yang berisi kunci.

Kunci

Kunci untuk pasangan kunci-nilai. Ini adalah urutan byte yang dikodekan UTF-8.

Nilai Panjang

Panjang nilai untuk pasangan kunci-nilai. Ini adalah nilai 2-byte ditafsirkan sebagai 16-bit unsigned integer yang menentukan jumlah byte yang berisi nilai.

Nilai

Nilai untuk pasangan kunci-nilai. Ini adalah urutan byte yang dikodekan UTF-8.

Hitungan Kunci Data Terenkripsi

Jumlah kunci data terenkripsi. Ini adalah nilai 2-byte yang ditafsirkan sebagai integer unsigned 16-bit yang menentukan jumlah kunci data terenkripsi. Jumlah maksimum kunci data terenkripsi di setiap pesan adalah 65.535 (2 ^ 16 - 1).

Kunci Data Terenkripsi

Urutan kunci data terenkripsi. Panjang urutan ditentukan oleh jumlah kunci data terenkripsi dan panjang masing-masing. Urutan berisi setidaknya satu kunci data terenkripsi.

Tabel berikut menjelaskan bidang yang membentuk setiap kunci data terenkripsi. Byte ditambahkan dalam urutan yang ditunjukkan.

Struktur Kunci Data Terenkripsi

Bidang	Panjang (byte)
Key Provider ID Length	2

Bidang	Panjang (byte)
Key Provider ID	Variabel. Sama dengan nilai yang ditentuka n dalam 2 byte sebelumnya (Panjang ID Penyedia Kunci).
Key Provider Information Length	2
Key Provider Information	Variabel. Sama dengan nilai yang ditentukan dalam 2 byte sebelumnya (Panjang Informasi Penyedia Kunci).
Encrypted Data Key Length	2
Encrypted Data Key	Variabel. Sama dengan nilai yang ditentuka n dalam 2 byte sebelumnya (Panjang Kunci Data Terenkripsi).

Panjang ID Penyedia Kunci

Panjang pengenal penyedia kunci. Ini adalah nilai 2-byte yang ditafsirkan sebagai integer unsigned 16-bit yang menentukan jumlah byte yang berisi ID penyedia kunci.

ID Penyedia Kunci

Pengidentifikasi penyedia kunci. Ini digunakan untuk menunjukkan penyedia kunci data terenkripsi dan dimaksudkan untuk dapat diperluas.

Panjang Informasi Penyedia Kunci

Panjang informasi penyedia kunci. Ini adalah nilai 2-byte yang ditafsirkan sebagai integer unsigned 16-bit yang menentukan jumlah byte yang berisi informasi penyedia kunci.

Informasi Penyedia Utama

Informasi penyedia utama. Itu ditentukan oleh penyedia kunci.

AWS KMS Kapan penyedia kunci utama atau Anda menggunakan AWS KMS keyring, nilai ini berisi Nama Sumber Daya Amazon (ARN) dari. AWS KMS key

Panjang Kunci Data Terenkripsi

Panjang kunci data terenkripsi. Ini adalah nilai 2-byte ditafsirkan sebagai 16-bit unsigned integer yang menentukan jumlah byte yang berisi kunci data terenkripsi.

Kunci Data Terenkripsi

Kunci data terenkripsi. Ini adalah kunci enkripsi data yang dienkripsi oleh penyedia kunci.

Jenis Konten

Jenis data terenkripsi, baik nonframed atau framed.

> **Note**
>
> Bila memungkinkan, gunakan data berbingkai. AWS Encryption SDK Mendukung data nonframed hanya untuk penggunaan lama. Beberapa implementasi bahasa masih AWS Encryption SDK dapat menghasilkan ciphertext nonframed. Semua implementasi bahasa yang didukung dapat mendekripsi ciphertext berbingkai dan nonframed.

Data berbingkai dibagi menjadi bagian yang sama panjangnya; setiap bagian dienkripsi secara terpisah. Konten berbingkai adalah tipe 2, dikodekan sebagai byte `02` dalam notasi heksadesimal.

Data nonframed tidak dibagi; itu adalah gumpalan terenkripsi tunggal. Konten non-framed adalah tipe 1, dikodekan sebagai byte `01` dalam notasi heksadesimal.

Dilindungi

Urutan cadangan 4 byte. Nilai ini harus 0. Ini dikodekan sebagai byte `00 00 00 00` dalam notasi heksadesimal (yaitu, urutan 4-byte dari nilai integer 32-bit sama dengan 0).

Bidang ini tidak ada dalam format pesan versi 2.

Panjang IV

Panjang vektor inisialisasi (IV). Ini adalah nilai 1-byte ditafsirkan sebagai 8-bit unsigned integer yang menentukan jumlah byte yang berisi IV. Nilai ini ditentukan oleh nilai IV byte dari algoritma yang menghasilkan pesan.

Bidang ini tidak ada dalam format pesan versi 2, yang hanya mendukung rangkaian algoritme yang menggunakan nilai IV deterministik di header pesan.

Panjang Bingkai

Panjang setiap frame data berbingkai. Ini adalah nilai 4-byte yang ditafsirkan sebagai integer unsigned 32-bit yang menentukan jumlah byte di setiap frame. Ketika data tidak dibingkai, yaitu, ketika nilai `Content Type` bidang adalah 1, nilai ini harus 0.

> **Note**
>
> Bila memungkinkan, gunakan data berbingkai. AWS Encryption SDK Mendukung data nonframed hanya untuk penggunaan lama. Beberapa implementasi bahasa masih AWS Encryption SDK dapat menghasilkan ciphertext nonframed. Semua implementasi bahasa yang didukung dapat mendekripsi ciphertext berbingkai dan nonframed.

Data Suite Algoritma

Data tambahan yang dibutuhkan oleh algoritma yang menghasilkan pesan. Panjang dan isi ditentukan oleh algoritma. Panjangnya mungkin 0.

Bidang ini tidak ada dalam format pesan versi 1.

Otentikasi Header

Otentikasi header ditentukan oleh algoritma yang menghasilkan pesan. Otentikasi header dihitung di seluruh header. Ini terdiri dari IV dan tag otentikasi. Byte ditambahkan dalam urutan yang ditunjukkan.

Struktur Otentikasi Header

Bidang	Panjang dalam versi 1.0 (byte)	Panjang dalam versi 2.0 (byte)
IV	Variabel. Ditentukan oleh nilai IV byte dari algoritma yang menghasilkan pesan.	N/A
Authentication Tag	Variabel. Ditentukan oleh nilai byte tag otentikasi dari algoritma yang menghasilkan pesan.	Variabel. Ditentukan oleh nilai byte tag otentikasi dari algoritma yang menghasilkan pesan.

IV

Vektor inisialisasi (IV) digunakan untuk menghitung tag otentikasi header.

Bidang ini tidak ada di header format pesan versi 2. Format pesan versi 2 hanya mendukung rangkaian algoritme yang menggunakan nilai IV deterministik di header pesan.

Tag Otentikasi

Nilai otentikasi untuk header. Ini digunakan untuk mengotentikasi seluruh isi header.

Struktur tubuh

Badan pesan berisi data terenkripsi, yang disebut ciphertext. Struktur tubuh tergantung pada jenis konten (tidak dibingkai atau dibingkai). Bagian berikut menjelaskan format badan pesan untuk setiap jenis konten. Struktur isi pesan sama dalam format pesan versi 1 dan 2.

Topik

- Data tidak dibingkai
- Data berbingkai

Data tidak dibingkai

Data non-frame dienkripsi dalam satu gumpalan dengan IV dan tubuh AAD yang unik.

> **Note**
>
> Bila memungkinkan, gunakan data berbingkai. AWS Encryption SDK Mendukung data nonframed hanya untuk penggunaan lama. Beberapa implementasi bahasa masih AWS Encryption SDK dapat menghasilkan ciphertext nonframed. Semua implementasi bahasa yang didukung dapat mendekripsi ciphertext berbingkai dan nonframed.

Tabel berikut menjelaskan bidang yang membentuk data nonframed. Byte ditambahkan dalam urutan yang ditunjukkan.

Struktur Tubuh Tidak Berbingkai

Bidang	Panjangnya, dalam byte
IV	Variabel. Sama dengan nilai yang ditentukan dalam IV Length byte header.
Encrypted Content Length	8
Encrypted Content	Variabel. Sama dengan nilai yang ditentuka n dalam 8 byte sebelumnya (Panjang Konten Terenkripsi).
Authentication Tag	Variabel. Ditentukan oleh implementasi algoritma yang digunakan.

IV

Vektor inisialisasi (IV) untuk digunakan dengan algoritma enkripsi.

Panjang Konten Terenkripsi

Panjang konten terenkripsi, atau ciphertext. Ini adalah nilai 8-byte yang ditafsirkan sebagai integer unsigned 64-bit yang menentukan jumlah byte yang berisi konten terenkripsi.

Secara teknis, nilai maksimum yang diizinkan adalah 2^63 - 1, atau 8 exbibytes (8 eIB). Namun, dalam praktiknya nilai maksimum adalah 2^36 - 32, atau 64 gibibytes (64 GiB), karena pembatasan yang diberlakukan oleh algoritma yang diterapkan.

> **Note**
>
> Implementasi Java SDK ini selanjutnya membatasi nilai ini menjadi 2^31 - 1, atau 2 gibibytes (2 GiB), karena pembatasan dalam bahasa.

Konten Terenkripsi

Konten terenkripsi (ciphertext) seperti yang dikembalikan oleh algoritma enkripsi.

Tag Otentikasi

Nilai otentikasi untuk tubuh. Ini digunakan untuk mengautentikasi badan pesan.

Data berbingkai

Dalam data berbingkai, data plaintext dibagi menjadi bagian yang sama panjangnya yang disebut frame. AWS Encryption SDK Enkripsi setiap frame secara terpisah dengan IV dan body AAD yang unik.

> **Note**
>
> Bila memungkinkan, gunakan data berbingkai. AWS Encryption SDK Mendukung data nonframed hanya untuk penggunaan lama. Beberapa implementasi bahasa masih AWS Encryption SDK dapat menghasilkan ciphertext nonframed. Semua implementasi bahasa yang didukung dapat mendekripsi ciphertext berbingkai dan nonframed.

Panjang bingkai, yang merupakan panjang konten terenkripsi dalam bingkai, dapat berbeda untuk setiap pesan. Jumlah maksimum byte dalam bingkai adalah 2^32 - 1. Jumlah maksimum frame dalam pesan adalah 2^32 - 1.

Ada dua jenis frame: reguler dan final. Setiap pesan harus terdiri dari atau menyertakan bingkai akhir.

Semua frame reguler dalam pesan memiliki panjang bingkai yang sama. Bingkai akhir dapat memiliki panjang bingkai yang berbeda.

Komposisi frame dalam data berbingkai bervariasi dengan panjang konten terenkripsi.

- Sama dengan panjang bingkai — Ketika panjang konten terenkripsi sama dengan panjang bingkai bingkai biasa, pesan dapat terdiri dari bingkai biasa yang berisi data, diikuti oleh bingkai akhir dengan panjang nol (0). Atau, pesan hanya dapat terdiri dari bingkai akhir yang berisi data. Dalam hal ini, frame akhir memiliki panjang frame yang sama dengan frame biasa.
- Kelipatan panjang bingkai — Ketika panjang konten terenkripsi adalah kelipatan yang tepat dari panjang bingkai bingkai biasa, pesan dapat berakhir dalam bingkai biasa yang berisi data, diikuti oleh bingkai akhir dengan panjang nol (0). Atau, pesan dapat berakhir dalam bingkai akhir yang berisi data. Dalam hal ini, frame akhir memiliki panjang frame yang sama dengan frame biasa.
- Bukan kelipatan dari panjang bingkai — Ketika panjang konten terenkripsi bukan kelipatan yang tepat dari panjang bingkai dari frame biasa, frame akhir berisi data yang tersisa. Panjang bingkai bingkai akhir kurang dari panjang bingkai bingkai biasa.

- Kurang dari panjang bingkai — Ketika panjang konten terenkripsi kurang dari panjang bingkai bingkai biasa, pesan terdiri dari bingkai akhir yang berisi semua data. Panjang bingkai bingkai akhir kurang dari panjang bingkai bingkai biasa.

Tabel berikut menjelaskan bidang yang membentuk bingkai. Byte ditambahkan dalam urutan yang ditunjukkan.

Struktur Tubuh Berbingkai, Bingkai Biasa

Bidang	Panjangnya, dalam byte
Sequence Number	4
IV	Variabel. Sama dengan nilai yang ditentukan dalam IV Length byte header.
Encrypted Content	Variabel. Sama dengan nilai yang ditentukan Frame Length dalam header.
Authentication Tag	Variabel. Ditentukan oleh algoritma yang digunakan, seperti yang Algorithm ID ditentuka n dalam header.

Nomor Urutan

Nomor urutan bingkai. Ini adalah nomor penghitung tambahan untuk bingkai. Ini adalah nilai 4-byte yang ditafsirkan sebagai bilangan bulat 32-bit yang tidak ditandatangani.

Data berbingkai harus dimulai dari nomor urut 1. Frame berikutnya harus berurutan dan harus berisi kenaikan 1 dari frame sebelumnya. Jika tidak, proses dekripsi berhenti dan melaporkan kesalahan.

IV

Vektor inisialisasi (IV) untuk frame. SDK menggunakan metode deterministik untuk membangun IV yang berbeda untuk setiap frame dalam pesan. Panjangnya ditentukan oleh rangkaian algoritma yang digunakan.

Konten Terenkripsi

Konten terenkripsi (ciphertext) untuk frame, seperti yang dikembalikan oleh algoritma enkripsi.

Tag Otentikasi

Nilai otentikasi untuk frame. Ini digunakan untuk mengotentikasi seluruh frame.

Struktur Tubuh Berbingkai, Bingkai Akhir

Bidang	Panjangnya, dalam byte
Sequence Number End	4
Sequence Number	4
IV	Variabel. Sama dengan nilai yang ditentukan dalam IV Length byte header.
Encrypted Content Length	4
Encrypted Content	Variabel. Sama dengan nilai yang ditentuka n dalam 4 byte sebelumnya (Panjang Konten Terenkripsi).
Authentication Tag	Variabel. Ditentukan oleh algoritma yang digunakan, seperti yang Algorithm ID ditentuka n dalam header.

Nomor Urutan Akhir

Indikator untuk frame akhir. Nilai dikodekan sebagai 4 byte `FF FF FF FF` dalam notasi heksadesimal.

Nomor Urutan

Nomor urutan bingkai. Ini adalah nomor penghitung tambahan untuk bingkai. Ini adalah nilai 4-byte yang ditafsirkan sebagai bilangan bulat 32-bit yang tidak ditandatangani.

Data berbingkai harus dimulai dari nomor urut 1. Frame berikutnya harus berurutan dan harus berisi kenaikan 1 dari frame sebelumnya. Jika tidak, proses dekripsi berhenti dan melaporkan kesalahan.

IV

Vektor inisialisasi (IV) untuk frame. SDK menggunakan metode deterministik untuk membangun IV yang berbeda untuk setiap frame dalam pesan. Panjang panjang IV ditentukan oleh rangkaian algoritma.

Panjang Konten Terenkripsi

Panjang konten terenkripsi. Ini adalah nilai 4-byte ditafsirkan sebagai 32-bit unsigned integer yang menentukan jumlah byte yang berisi konten terenkripsi untuk frame.

Konten Terenkripsi

Konten terenkripsi (ciphertext) untuk frame, seperti yang dikembalikan oleh algoritma enkripsi.

Tag Otentikasi

Nilai otentikasi untuk frame. Ini digunakan untuk mengotentikasi seluruh frame.

Struktur footer

Ketika algoritma dengan penandatanganan digunakan, format pesan berisi footer. Footer pesan berisi tanda tangan digital yang dihitung melalui header dan isi pesan. Tabel berikut menjelaskan bidang yang membentuk footer. Byte ditambahkan dalam urutan yang ditunjukkan. Struktur footer pesan sama dalam format pesan versi 1 dan 2.

Struktur Footer

Bidang	Panjangnya, dalam byte
Signature Length	2
Signature	Variabel. Sama dengan nilai yang ditentuka n dalam 2 byte sebelumnya (Panjang Tanda Tangan).

Panjang Tanda Tangan

Panjang tanda tangan. Ini adalah nilai 2-byte ditafsirkan sebagai 16-bit unsigned integer yang menentukan jumlah byte yang berisi tanda tangan.

Tanda tangan

Tanda tangan.

AWS Encryption SDK contoh format pesan

Informasi di halaman ini adalah referensi untuk membangun pustaka enkripsi Anda sendiri yang kompatibel dengan file AWS Encryption SDK. Jika Anda tidak membangun pustaka enkripsi kompatibel Anda sendiri, Anda mungkin tidak memerlukan informasi ini.

Untuk menggunakan AWS Encryption SDK dalam salah satu bahasa pemrograman yang didukung, lihatBahasa pemrograman.

Untuk spesifikasi yang mendefinisikan elemen AWS Encryption SDK implementasi yang tepat, lihat AWS Encryption SDK Spesifikasi di GitHub.

Topik berikut menunjukkan contoh format AWS Encryption SDK pesan. Setiap contoh menunjukkan byte mentah, dalam notasi heksadesimal, diikuti dengan deskripsi tentang apa yang diwakili oleh byte tersebut.

Topik

- Data berbingkai (format pesan versi 1)
- Data berbingkai (format pesan versi 2)
- Data yang tidak dibingkai (format pesan versi 1)

Data berbingkai (format pesan versi 1)

Contoh berikut menunjukkan format pesan untuk data berbingkai dalam format pesan versi 1.

```
+--------+
| Header |
+--------+
01                                      Version (1.0)
80                                      Type (128, customer authenticated encrypted
 data)
0378                                    Algorithm ID (see Referensi algoritma)
6E7C0FBD 4DF4A999 717C22A2 DDFE1A27     Message ID (random 128-bit value)
```

```
008E                                    AAD Length (142)
0004                                    AAD Key-Value Pair Count (4)
0005                                    AAD Key-Value Pair 1, Key Length (5)
30746869 73                             AAD Key-Value Pair 1, Key ("0This")
0002                                    AAD Key-Value Pair 1, Value Length (2)
6973                                    AAD Key-Value Pair 1, Value ("is")
0003                                    AAD Key-Value Pair 2, Key Length (3)
31616E                                  AAD Key-Value Pair 2, Key ("1an")
000A                                    AAD Key-Value Pair 2, Value Length (10)
656E6372 79774690 6F6E                  AAD Key-Value Pair 2, Value ("encryption")
0008                                    AAD Key-Value Pair 3, Key Length (8)
32636F6E 74657874                       AAD Key-Value Pair 3, Key ("2context")
0007                                    AAD Key-Value Pair 3, Value Length (7)
6578616D 706C65                         AAD Key-Value Pair 3, Value ("example")
0015                                    AAD Key-Value Pair 4, Key Length (21)
6177732D 63727970 746F2D70 75626C69     AAD Key-Value Pair 4, Key ("aws-crypto-
public-key")
632D6B65 79
0044                                    AAD Key-Value Pair 4, Value Length (68)
416A4173 7569326F 7430364C 4B77715A     AAD Key-Value Pair 4, Value
 ("AjAsui2ot06LKwqZXDJnU/Aqc2vD+0OkpOZ1cc8Tg2qd7rs5aLTg7lvfUEW/86+/5w==")
58444A6E 552F4171 63327644 2B304F6B
704F5A31 63633854 67327164 37727335
614C5467 376C7666 5545572F 38362B2F
35773D3D
0002                                    EncryptedDataKeyCount (2)
0007                                    Encrypted Data Key 1, Key Provider ID Length
 (7)
6177732D 6B6D73                         Encrypted Data Key 1, Key Provider ID ("aws-
kms")
004B                                    Encrypted Data Key 1, Key Provider
 Information Length (75)
61726E3A 6177733A 6B6D733A 75732D77      Encrypted Data Key 1, Key Provider
 Information ("arn:aws:kms:us-west-2:111122223333:key/715c0818-5825-4245-
a755-138a6d9a11e6")
6573742D 323A3131 31313232 32323333
33333A6B 65792F37 31356330 3831382D
35383235 2D343234 352D6137 35352D31
33386136 64396131 316536
00A7                                    Encrypted Data Key 1, Encrypted Data Key
 Length (167)
01010200 7857A1C1 F7370545 4ECA7C83      Encrypted Data Key 1, Encrypted Data Key
956C4702 23DCE8D7 16C59679 973E3CED
02A4EF29 7F000000 7E307C06 092A8648
```

```
86F70D01 0706A06F 306D0201 00306806
092A8648 86F70D01 0701301E 06096086
48016503 04012E30 11040C3F F02C897B
7A12EB19 8BF2D802 0110803B 24003D1F
A5474FBC 392360B5 CB9997E0 6A17DE4C
A6BD7332 6BF86DAB 60D8CCB8 8295DBE9
4707E356 ADA3735A 7C52D778 B3135A47
9F224BF9 E67E87
0007                                    Encrypted Data Key 2, Key Provider ID Length
 (7)
6177732D 6B6D73                         Encrypted Data Key 2, Key Provider ID ("aws-
kms")
004E                                    Encrypted Data Key 2, Key Provider
 Information Length (78)
61726E3A 6177733A 6B6D733A 63612D63      Encrypted Data Key 2, Key Provider
 Information ("arn:aws:kms:ca-central-1:111122223333:key/9b13ca4b-afcc-46a8-aa47-
be3435b423ff")
656E7472 616C2D31 3A313131 31323232
32333333 333A6B65 792F3962 31336361
34622D61 6663632D 34366138 2D616134
372D6265 33343335 62343233 6666
00A7                                    Encrypted Data Key 2, Encrypted Data Key
 Length (167)
01010200 78FAFFFB D6DE06AF AC72F79B      Encrypted Data Key 2, Encrypted Data Key
0E57BD87 3F60F4E6 FD196144 5A002C94
AF787150 69000000 7E307C06 092A8648
86F70D01 0706A06F 306D0201 00306806
092A8648 86F70D01 0701301E 06096086
48016503 04012E30 11040C36 CD985E12
D218B674 5BBC6102 0110803B 0320E3CD
E470AA27 DEAB660B 3E0CE8E0 8B1A89E4
57DCC69B AAB1294F 21202C01 9A50D323
72EBAAFD E24E3ED8 7168E0FA DB40508F
556FBD58 9E621C
02                                      Content Type (2, framed data)
00000000                                Reserved
0C                                      IV Length (12)
00000100                                Frame Length (256)
4ECBD5C0 9899CA65 923D2347              IV
0B896144 0CA27950 CA571201 4DA58029      Authentication Tag
+------+
| Body |
+------+
00000001                                Frame 1, Sequence Number (1)
```

```
6BD3FE9C ADBCB213 5B89E8F1                Frame 1, IV
1F6471E0 A51AF310 10FA9EF6 F0C76EDF       Frame 1, Encrypted Content
F5AFA33C 7D2E8C6C 9C5D5175 A212AF8E
FBD9A0C3 C6E3FB59 C125DBF2 89AC7939
BDEE43A8 0F00F49E ACBBD8B2 1C785089
A90DB923 699A1495 C3B31B50 0A48A830
201E3AD9 1EA6DA14 7F6496DB 6BC104A4
DEB7F372 375ECB28 9BF84B6D 2863889F
CB80A167 9C361C4B 5EC07438 7A4822B4
A7D9D2CC 5150D414 AF75F509 FCE118BD
6D1E798B AEBA4CDB AD009E5F 1A571B77
0041BC78 3E5F2F41 8AF157FD 461E959A
BB732F27 D83DC36D CC9EBC05 00D87803
57F2BB80 066971C2 DEEA062F 4F36255D
E866C042 E1382369 12E9926B BA40E2FC
A820055F FB47E428 41876F14 3B6261D9
5262DB34 59F5D37E 76E46522 E8213640
04EE3CC5 379732B5 F56751FA 8E5F26AD       Frame 1, Authentication Tag
00000002                                  Frame 2, Sequence Number (2)
F1140984 FF25F943 959BE514                Frame 2, IV
216C7C6A 2234F395 F0D2D9B9 304670BF       Frame 2, Encrypted Content
A1042608 8A8BCB3F B58CF384 D72EC004
A41455B4 9A78BAC9 36E54E68 2709B7BD
A884C1E1 705FF696 E540D297 446A8285
23DFEE28 E74B225A 732F2C0C 27C6BDA2
7597C901 65EF3502 546575D4 6D5EBF22
1FF787AB 2E38FD77 125D129C 43D44B96
778D7CEE 3C36625F FF3A985C 76F7D320
ED70B1F3 79729B47 E7D9B5FC 02FCE9F5
C8760D55 7779520A 81D54F9B EC45219D
95941F7E 5CBAEAC8 CEC13B62 1464757D
AC65B6EF 08262D74 44670624 A3657F7F
2A57F1FD E7060503 AC37E197 2F297A84
DF1172C2 FA63CF54 E6E2B9B6 A86F582B
3B16F868 1BBC5E4D 0B6919B3 08D5ABCF
FECDC4A4 8577F08B 99D766A1 E5545670
A61F0A3B A3E45A84 4D151493 63ECA38F       Frame 2, Authentication Tag
FFFFFFFF                                  Final Frame, Sequence Number End
00000003                                  Final Frame, Sequence Number (3)
35F74F11 25410F01 DD9E04BF                Final Frame, IV
0000008E                                  Final Frame, Encrypted Content Length (142)
F7A53D37 2F467237 6FBD0B57 D1DFE830       Final Frame, Encrypted Content
B965AD1F A910AA5F 5EFFFFF4 BC7D431C
BA9FA7C4 B25AF82E 64A04E3A A0915526
```

```
88859500 7096FABB 3ACAD32A 75CFED0C
4A4E52A3 8E41484D 270B7A0F ED61810C
3A043180 DF25E5C5 3676E449 0986557F
C051AD55 A437F6BC 139E9E55 6199FD60
6ADC017D BA41CDA4 C9F17A83 3823F9EC
B66B6A5A 80FDB433 8A48D6A4 21CB
811234FD 8D589683 51F6F39A 040B3E3B        Final Frame, Authentication Tag
+--------+
| Footer |
+--------+
0066                                       Signature Length (102)
30640230 085C1D3C 63424E15 B2244448        Signature
639AED00 F7624854 F8CF2203 D7198A28
758B309F 5EFD9D5D 2E07AD0B 467B8317
5208B133 02301DF7 2DFC877A 66838028
3C6A7D5E 4F8B894E 83D98E7C E350F424
7E06808D 0FE79002 E24422B9 98A0D130
A13762FF 844D
```

Data berbingkai (format pesan versi 2)

Contoh berikut menunjukkan format pesan untuk data berbingkai dalam format pesan versi 2.

```
+--------+
| Header |
+--------+
02                                         Version (2.0)
0578                                       Algorithm ID (see Algorithms reference)
122747eb 21dfe39b 38631c61 7fad7340
cc621a30 32a11cc3 216d0204 fd148459        Message ID (random 256-bit value)
008e                                       AAD Length (142)
0004                                       AAD Key-Value Pair Count (4)
0005                                       AAD Key-Value Pair 1, Key Length (5)
30546869 73                                AAD Key-Value Pair 1, Key ("0This")
0002                                       AAD Key-Value Pair 1, Value Length (2)
6973                                       AAD Key-Value Pair 1, Value ("is")
0003                                       AAD Key-Value Pair 2, Key Length (3)
31616e                                     AAD Key-Value Pair 2, Key ("1an")
000a                                       AAD Key-Value Pair 2, Value Length (10)
656e6372 79707469 6f6e                     AAD Key-Value Pair 2, Value ("encryption")
0008                                       AAD Key-Value Pair 3, Key Length (8)
32636f6e 74657874                          AAD Key-Value Pair 3, Key ("2context")
0007                                       AAD Key-Value Pair 3, Value Length (7)
```

```
6578616d 706c65                          AAD Key-Value Pair 3, Value ("example")
0015                                     AAD Key-Value Pair 4, Key Length (21)
6177732d 63727970 746f2d70 75626c69      AAD Key-Value Pair 4, Key ("aws-crypto-
public-key")
632d6b65 79
0044                                     AAD Key-Value Pair 4, Value Length (68)
41746733 72703845 41345161 36706669      AAD Key-Value Pair 4, Value
 ("QXRnM3JwOEVBNFFhNnBmaTk3MUlTNTk3NHpOMnlZWE5vSmtwRHFPc0dIYkVaVDRqME5OMlFkRStmbTFVY01WdThnPT0=
39373149 53353937 347a4e32 7959584e
6f4a6b70 44714f73 47486245 5a54346a
304e4e32 5164452b 666d3155 634d5675
38673d3d
0001                                     Encrypted Data Key Count (1)
0007                                     Encrypted Data Key 1, Key Provider ID Length
 (7)
6177732d 6b6d73                          Encrypted Data Key 1, Key Provider ID ("aws-
kms")
004b                                     Encrypted Data Key 1, Key Provider
 Information Length (75)
61726e3a 6177733a 6b6d733a 75732d77       Encrypted Data Key 1, Key
 Provider Information ("arn:aws:kms:us-west-2:658956600833:key/b3537ef1-
d8dc-4780-9f5a-55776cbb2f7f")
6573742d 323a3635 38393536 36303038
33333a6b 65792f62 33353337 6566312d
64386463 2d343738 302d3966 35612d35
35373736 63626232 663766
00a7                                     Encrypted Data Key 1, Encrypted Data Key
 Length (167)
01010100 7840f38c 275e3109 7416c107      Encrypted Data Key 1, Encrypted Data Key
29515057 1964ada3 ef1c21e9 4c8ba0bd
bc9d0fb4 14000000 7e307c06 092a8648
86f70d01 0706a06f 306d0201 00306806
092a8648 86f70d01 0701301e 06096086
48016503 04012e30 11040c39 32d75294
06063803 f8460802 0110803b 2a46bc23
413196d2 903bf1d7 3ed98fc8 a94ac6ed
e00ee216 74ec1349 12777577 7fa052a5
ba62e9e4 f2ac8df6 bcb1758f 2ce0fb21
cc9ee5c9 7203bb
02                                       Content Type (2, framed data)
00001000                                 Frame Length (4096)
05cd035b 29d5499d 4587570b 87502afe      Algorithm Suite Data (key commitment)
634f7b2c c3df2aa9 88a10105 4a2c7687
76cb339f 2536741f 59a1c202 4f2594ab      Authentication Tag
```

```
+------+
| Body |
+------+
ffffffff                                Final Frame, Sequence Number End
00000001                                Final Frame, Sequence Number (1)
00000000 00000000 00000001              Final Frame, IV
00000009                                Final Frame, Encrypted Content Length (9)
fa6e39c6 02927399 3e                    Final Frame, Encrypted Content
f683a564 405d68db eeb0656c d57c9eb0      Final Frame, Authentication Tag
+--------+
| Footer |
+--------+
0067                                    Signature Length (103)
30650230 2a1647ad 98867925 c1712e8f      Signature
ade70b3f 2a2bc3b8 50eb91ef 56cfdd18
967d91d8 42d92baf 357bba48 f636c7a0
869cade2 023100aa ae12d08f 8a0afe85
e5054803 110c9ed8 11b2e08a c4a052a9
074217ea 3b01b660 534ac921 bf091d12
3657e2b0 9368bd
```

Data yang tidak dibingkai (format pesan versi 1)

Contoh berikut menunjukkan format pesan untuk data nonframed.

> **Note**
>
> Bila memungkinkan, gunakan data berbingkai. AWS Encryption SDK Mendukung data nonframed hanya untuk penggunaan lama. Beberapa implementasi bahasa masih AWS Encryption SDK dapat menghasilkan ciphertext nonframed. Semua implementasi bahasa yang didukung dapat mendekripsi ciphertext berbingkai dan nonframed.

```
+--------+
| Header |
+--------+
01                                      Version (1.0)
80                                      Type (128, customer authenticated encrypted
 data)
0378                                    Algorithm ID (see Referensi algoritma)
B8929B01 753D4A45 C0217F39 404F70FF      Message ID (random 128-bit value)
```

```
008E                                    AAD Length (142)
0004                                    AAD Key-Value Pair Count (4)
0005                                    AAD Key-Value Pair 1, Key Length (5)
30746869 73                             AAD Key-Value Pair 1, Key ("0This")
0002                                    AAD Key-Value Pair 1, Value Length (2)
6973                                    AAD Key-Value Pair 1, Value ("is")
0003                                    AAD Key-Value Pair 2, Key Length (3)
31616E                                  AAD Key-Value Pair 2, Key ("1an")
000A                                    AAD Key-Value Pair 2, Value Length (10)
656E6372 79774690 6F6E                  AAD Key-Value Pair 2, Value ("encryption")
0008                                    AAD Key-Value Pair 3, Key Length (8)
32636F6E 74657874                       AAD Key-Value Pair 3, Key ("2context")
0007                                    AAD Key-Value Pair 3, Value Length (7)
6578616D 706C65                         AAD Key-Value Pair 3, Value ("example")
0015                                    AAD Key-Value Pair 4, Key Length (21)
6177732D 63727970 746F2D70 75626C69     AAD Key-Value Pair 4, Key ("aws-crypto-
public-key")
632D6B65 79
0044                                    AAD Key-Value Pair 4, Value Length (68)
41734738 67473949 6E4C5075 3136594B     AAD Key-Value Pair 4, Value
 ("AsG8gG9InLPu16YKlqXTOD+nykG8YqHAhqecj8aXfD2e5B4gtVE73dZkyClA+rAMOQ==")
6C715854 4F442B6E 796B4738 59714841
68716563 6A386158 66443265 35423467
74564537 33645A6B 79436C41 2B72414D
4F513D3D
0002                                    Encrypted Data Key Count (2)
0007                                    Encrypted Data Key 1, Key Provider ID Length
 (7)
6177732D 6B6D73                         Encrypted Data Key 1, Key Provider ID ("aws-
kms")
004B                                    Encrypted Data Key 1, Key Provider
 Information Length (75)
61726E3A 6177733A 6B6D733A 75732D77     Encrypted Data Key 1, Key Provider
 Information ("arn:aws:kms:us-west-2:111122223333:key/715c0818-5825-4245-
a755-138a6d9a11e6")
6573742D 323A3131 31313232 32323333
33333A6B 65792F37 31356330 3831382D
35383235 2D343234 352D6137 35352D31
33386136 64396131 316536
00A7                                    Encrypted Data Key 1, Encrypted Data Key
 Length (167)
01010200 7857A1C1 F7370545 4ECA7C83     Encrypted Data Key 1, Encrypted Data Key
956C4702 23DCE8D7 16C59679 973E3CED
02A4EF29 7F000000 7E307C06 092A8648
```

```
86F70D01 0706A06F 306D0201 00306806
092A8648 86F70D01 0701301E 06096086
48016503 04012E30 11040C28 4116449A
0F2A0383 659EF802 0110803B B23A8133
3A33605C 48840656 C38BCB1F 9CCE7369
E9A33EBE 33F46461 0591FECA 947262F3
418E1151 21311A75 E575ECC5 61A286E0
3E2DEBD5 CB005D
0007                                    Encrypted Data Key 2, Key Provider ID Length
 (7)
6177732D 6B6D73                         Encrypted Data Key 2, Key Provider ID ("aws-
kms")
004E                                    Encrypted Data Key 2, Key Provider
 Information Length (78)
61726E3A 6177733A 6B6D733A 63612D63      Encrypted Data Key 2, Key Provider
 Information ("arn:aws:kms:ca-central-1:111122223333:key/9b13ca4b-afcc-46a8-aa47-
be3435b423ff")
656E7472 616C2D31 3A313131 31323232
32333333 333A6B65 792F3962 31336361
34622D61 6663632D 34366138 2D616134
372D6265 33343335 62343233 6666
00A7                                    Encrypted Data Key 2, Encrypted Data Key
 Length (167)
01010200 78FAFFFB D6DE06AF AC72F79B      Encrypted Data Key 2, Encrypted Data Key
0E57BD87 3F60F4E6 FD196144 5A002C94
AF787150 69000000 7E307C06 092A8648
86F70D01 0706A06F 306D0201 00306806
092A8648 86F70D01 0701301E 06096086
48016503 04012E30 11040CB2 A820D0CC
76616EF2 A6B30D02 0110803B 8073D0F1
FDD01BD9 B0979082 099FDBFC F7B13548
3CC686D7 F3CF7C7A CCC52639 122A1495
71F18A46 80E2C43F A34C0E58 11D05114
2A363C2A E11397
01                                      Content Type (1, nonframed data)
00000000                                Reserved
0C                                      IV Length (12)
00000000                                Frame Length (0, nonframed data)
734C1BBE 032F7025 84CDA9D0              IV
2C82BB23 4CBF4AAB 8F5C6002 622E886C      Authentication Tag
+------+
| Body |
+------+
D39DD3E5 915E0201 77A4AB11              IV
```

```
00000000 0000028E                           Encrypted Content Length (654)
E8B6F955 B5F22FE4 FD890224 4E1D5155         Encrypted Content
5871BA4C 93F78436 1085E4F8 D61ECE28
59455BD8 D76479DF C28D2E0B BDB3D5D3
E4159DFE C8A944B6 685643FC EA24122B
6766ECD5 E3F54653 DF205D30 0081D2D8
55FCDA5B 9F5318BC F4265B06 2FE7C741
C7D75BCC 10F05EA5 0E2F2F40 47A60344
ECE10AA7 559AF633 9DE2C21B 12AC8087
95FE9C58 C65329D1 377C4CD7 EA103EC1
31E4F48A 9B1CC047 EE5A0719 704211E5
B48A2068 8060DF60 B492A737 21B0DB21
C9B21A10 371E6179 78FAFB0B BAAEC3F4
9D86E334 701E1442 EA5DA288 64485077
54C0C231 AD43571A B9071925 609A4E59
B8178484 7EB73A4F AAE46B26 F5B374B8
12B0000C 8429F504 936B2492 AAF47E94
A5BA804F 7F190927 5D2DF651 B59D4C2F
A15D0551 DAEBA4AF 2060D0D5 CB1DA4E6
5E2034DB 4D19E7CD EEA6CF7E 549C86AC
46B2C979 AB84EE12 202FD6DF E7E3C09F
C2394012 AF20A97E 369BCBDA 62459D3E
C6FFB914 FEFD4DE5 88F5AFE1 98488557
1BABBAE4 BE55325E 4FB7E602 C1C04BEE
F3CB6B86 71666C06 6BF74E1B 0F881F31
B731839B CF711F6A 84CA95F5 958D3B44
E3862DF6 338E02B5 C345CFF8 A31D54F3
6920AA76 0BF8E903 552C5A04 917CCD11
D4E5DF5C 491EE86B 20C33FE1 5D21F0AD
6932E67C C64B3A26 B8988B25 CFA33E2B
63490741 3AB79D60 D8AEFBE9 2F48E25A
978A019C FE49EE0A 0E96BF0D D6074DDB
66DFF333 0E10226F 0A1B219C BE54E4C2
2C15100C 6A2AA3F1 88251874 FDC94F6B
9247EF61 3E7B7E0D 29F3AD89 FA14A29C
76E08E9B 9ADCDF8C C886D4FD A69F6CB4
E24FDE26 3044C856 BF08F051 1ADAD329
C4A46A1E B5AB72FE 096041F1 F3F3571B
2EAFD9CB B9EB8B83 AE05885A 8F2D2793
1E3305D9 0C9E2294 E8AD7E3B 8E4DEC96
6276C5F1 A3B7E51E 422D365D E4C0259C
50715406 822D1682 80B0F2E5 5C94
65B2E942 24BEEA6E A513F918 CCEC1DE3      Authentication Tag
+--------+
```

```
| Footer |
+--------+
0067                                    Signature Length (103)
30650230 7229DDF5 B86A5B64 54E4D627     Signature
CBE194F1 1CC0F8CF D27B7F8B F50658C0
BE84B355 3CED1721 A0BE2A1B 8E3F449E
1BEB8281 023100B2 0CB323EF 58A4ACE3
1559963B 889F72C3 B15D1700 5FB26E61
331F3614 BC407CEE B86A66FA CBF74D9E
34CB7E4B 363A38
```

Referensi data terautentikasi tambahan badan (AAD) untuk AWS Encryption SDK

Informasi di halaman ini adalah referensi untuk membangun pustaka enkripsi Anda sendiri yang kompatibel dengan file AWS Encryption SDK. Jika Anda tidak membangun pustaka enkripsi kompatibel Anda sendiri, Anda mungkin tidak memerlukan informasi ini.

Untuk menggunakan AWS Encryption SDK dalam salah satu bahasa pemrograman yang didukung, lihatBahasa pemrograman.

Untuk spesifikasi yang mendefinisikan elemen AWS Encryption SDK implementasi yang tepat, lihat AWS Encryption SDK Spesifikasi di GitHub.

Anda harus memberikan data otentikasi tambahan (AAD) ke algoritma AES-GCM untuk setiap operasi kriptografi. Ini berlaku untuk data tubuh berbingkai dan tidak berbingkai. Untuk informasi selengkapnya tentang AAD dan cara penggunaannya dalam Galois/Counter Mode (GCM), lihat Rekomendasi untuk Mode Operasi Sandi Blok: Galois/Counter Mode (GCM) dan GMAC.

Tabel berikut menjelaskan bidang yang membentuk tubuh AAD. Byte ditambahkan dalam urutan yang ditunjukkan.

Struktur AAD Tubuh

Bidang	Panjangnya, dalam byte
Message ID	16

Bidang	Panjangnya, dalam byte
Body AAD Content	Variabel. Lihat Konten Body AAD dalam daftar berikut.
Sequence Number	4
Content Length	8

ID Pesan

Message IDNilai yang sama ditetapkan dalam header pesan.

Konten AAD Tubuh

Nilai yang dikodekan UTF-8 ditentukan oleh jenis data tubuh yang digunakan.

Untuk data nonframed, gunakan nilainya. `AWSKMSEncryptionClient Single Block`

Untuk frame reguler dalam data berbingkai, gunakan nilainya`AWSKMSEncryptionClient Frame`.

Untuk frame terakhir dalam data berbingkai, gunakan nilainya`AWSKMSEncryptionClient Final Frame`.

Nomor Urutan

Sebuah nilai 4-byte ditafsirkan sebagai 32-bit unsigned integer.

Untuk data berbingkai, ini adalah nomor urut bingkai.

Untuk data nonframed, gunakan nilai 1, dikodekan sebagai 4 byte `00 00 00 01` dalam notasi heksadesimal.

Panjang Konten

Panjang, dalam byte, dari data plaintext yang disediakan untuk algoritma untuk enkripsi. Ini adalah nilai 8-byte yang ditafsirkan sebagai integer unsigned 64-bit.

AWS Encryption SDK referensi algoritma

Informasi di halaman ini adalah referensi untuk membangun pustaka enkripsi Anda sendiri yang kompatibel dengan file AWS Encryption SDK. Jika Anda tidak membangun pustaka enkripsi kompatibel Anda sendiri, Anda mungkin tidak memerlukan informasi ini.

Untuk menggunakan AWS Encryption SDK dalam salah satu bahasa pemrograman yang didukung, lihatBahasa pemrograman.

Untuk spesifikasi yang mendefinisikan elemen AWS Encryption SDK implementasi yang tepat, lihat AWS Encryption SDK Spesifikasi di GitHub.

Jika Anda membangun perpustakaan Anda sendiri yang dapat membaca dan menulis ciphertext yang kompatibel dengan AWS Encryption SDK, Anda harus memahami bagaimana AWS Encryption SDK mengimplementasikan suite algoritme yang didukung untuk mengenkripsi data mentah.

AWS Encryption SDK Mendukung suite algoritma berikut. Semua suite algoritma AES-GCM memiliki vektor inisialisasi 12-byte dan tag otentikasi AES-GCM 16-byte. Rangkaian algoritme default bervariasi sesuai dengan AWS Encryption SDK versi dan kebijakan komitmen kunci yang dipilih. Untuk detailnya, lihat Kebijakan komitmen dan rangkaian algoritme.

AWS Encryption SDK Suite Algoritma

ID Algoritma	Versi format pesan	Enkripsi algoritme	Panjang kunci data (bit)	Algoritma derivasi kunci	Algoritma tanda tangan	Algoritma komitmen utama	Panjang data rangkaian algoritma (byte)
05 78	0x02	AES-GCM	256	HKDF dengan SHA-512	ECDSA dengan P-384 dan SHA-384	HKDF dengan SHA-512	32 (komitmen utama)

ID Algoritma	Versi format pesan	Enkripsi algoritme	Panjang kunci data (bit)	Algoritma derivasi kunci	Algoritma tanda tangan	Algoritma komitmen utama	Panjang data rangkaian algoritma (byte)
04 78	0x02	AES-GCM	256	HKDF dengan SHA-512	Tidak ada	HKDF dengan SHA-512	32 (komitmen utama)
03 78	0x01	AES-GCM	256	HKDF dengan SHA-384	ECDSA dengan P-384 dan SHA-384	Tidak ada	N/A
03 46	0x01	AES-GCM	192	HKDF dengan SHA-384	ECDSA dengan P-384 dan SHA-384	Tidak ada	N/A
02 14	0x01	AES-GCM	128	HKDF dengan SHA-256	ECDSA dengan P-256 dan SHA-256	Tidak ada	N/A
01 78	0x01	AES-GCM	256	HKDF dengan SHA-256	Tidak ada	Tidak ada	N/A
01 46	0x01	AES-GCM	192	HKDF dengan SHA-256	Tidak ada	Tidak ada	N/A

ID Algoritma	Versi format pesan	Enkripsi algoritme	Panjang kunci data (bit)	Algoritma derivasi kunci	Algoritma tanda tangan	Algoritma komitmen utama	Panjang data rangkaian algoritma (byte)
`01 14`	0x01	AES-GCM	128	HKDF dengan SHA-256	Tidak ada	Tidak ada	N/A
`00 78`	0x01	AES-GCM	256	Tidak ada	Tidak ada	Tidak ada	N/A
`00 46`	0x01	AES-GCM	192	Tidak ada	Tidak ada	Tidak ada	N/A
`00 14`	0x01	AES-GCM	128	Tidak ada	Tidak ada	Tidak ada	N/A

ID Algoritma

Nilai heksadesimal 2-byte yang secara unik mengidentifikasi implementasi algoritma. Nilai ini disimpan di header pesan ciphertext.

Versi format pesan

Versi format pesan. Suite algoritma dengan komitmen utama menggunakan format pesan versi 2 (0x02). Suite algoritma tanpa komitmen kunci menggunakan format pesan versi 1 (0x01).

Panjang data rangkaian algoritma

Panjang dalam byte data khusus untuk suite algoritma. Bidang ini hanya didukung dalam format pesan versi 2 (0x02). Dalam format pesan versi 2 (0x02), data ini muncul di `Algorithm suite data` bidang header pesan. Rangkaian algoritma yang mendukung komitmen kunci menggunakan 32 byte untuk string komitmen utama. Untuk informasi selengkapnya, lihat Algoritma komitmen utama dalam daftar ini.

Panjang kunci data

Panjang kunci data dalam bit. AWS Encryption SDK Mendukung kunci 256-bit, 192-bit, dan 128-bit. Kunci data dihasilkan oleh keyring atau kunci master.

Dalam beberapa implementasi, kunci data ini digunakan sebagai masukan ke fungsi derivasi extract-and-expand kunci berbasis HMAC (HKDF). Output dari HKDF digunakan sebagai kunci enkripsi data dalam algoritma enkripsi. Untuk informasi selengkapnya, lihat Algoritma derivasi kunci dalam daftar ini.

Enkripsi algoritme

Nama dan mode algoritma enkripsi yang digunakan. Suite algoritma dalam AWS Encryption SDK menggunakan algoritma enkripsi Advanced Encryption Standard (AES) dengan Galois/Counter Mode (GCM).

Algoritma komitmen utama

Algoritma yang digunakan untuk menghitung string komitmen kunci. Output disimpan di `Algorithm suite data` bidang header pesan dan digunakan untuk memvalidasi kunci data untuk komitmen utama.

Untuk penjelasan teknis tentang menambahkan komitmen utama ke rangkaian algoritme, lihat Key Committing AEADs in Cryptology ePrint Archive.

Algoritma derivasi kunci

Fungsi derivasi extract-and-expand kunci berbasis HMAC (HKDF) digunakan untuk menurunkan kunci enkripsi data. AWS Encryption SDK Penggunaan HKDF didefinisikan dalam RFC 5869.

Suite algoritma tanpa komitmen kunci (ID algoritma `01xx` —`03xx`)

- Fungsi hash yang digunakan adalah SHA-384 atau SHA-256, tergantung pada rangkaian algoritma.
- Untuk langkah ekstrak:
  - Tidak ada garam yang digunakan. Per RFC, garam diatur ke string nol. Panjang string sama dengan panjang output fungsi hash, yaitu 48 byte untuk SHA-384 dan 32 byte untuk SHA-256.
  - Materi kunci input adalah kunci data dari keyring atau penyedia kunci master.
- Untuk langkah perluasan:
  - Kunci pseudorandom input adalah output dari langkah ekstrak.
  - Info input adalah gabungan dari ID algoritma dan ID pesan (dalam urutan itu).
  - Panjang bahan kunci keluaran adalah panjang kunci Data. Output ini digunakan sebagai kunci enkripsi data dalam algoritma enkripsi.

Suite algoritma dengan komitmen utama (ID algoritma `04xx` dan`05xx`)

- Fungsi hash yang digunakan adalah SHA-512.
- Untuk langkah ekstrak:
  - Garam adalah nilai acak kriptografi 256-bit. Dalam format pesan versi 2 (0x02), nilai ini disimpan di lapangan. `MessageID`
  - Materi kunci awal adalah kunci data dari keyring atau penyedia kunci master.
- Untuk langkah perluasan:
  - Kunci pseudorandom input adalah output dari langkah ekstrak.
  - Label kuncinya adalah byte yang dikodekan UTF-8 dari `DERIVEKEY` string dalam urutan byte endian besar.
  - Info input adalah gabungan dari ID algoritma dan label kunci (dalam urutan itu).
  - Panjang bahan kunci keluaran adalah panjang kunci Data. Output ini digunakan sebagai kunci enkripsi data dalam algoritma enkripsi.

Versi format pesan

Versi format pesan yang digunakan dengan suite algoritma. Lihat perinciannya di Referensi format pesan.

Algoritma tanda tangan

Algoritma tanda tangan yang digunakan untuk menghasilkan tanda tangan digital di atas header dan body ciphertext. AWS Encryption SDK Menggunakan Elliptic Curve Digital Signature Algorithm (ECDSA) dengan spesifikasi sebagai berikut:

- Kurva elips yang digunakan adalah kurva P-384 atau P-256, seperti yang ditentukan oleh ID algoritma. Kurva ini didefinisikan dalam Digital Signature Standard (DSS) (FIPS PUB 186-4).
- Fungsi hash yang digunakan adalah SHA-384 (dengan kurva P-384) atau SHA-256 (dengan kurva P-256).

AWS Encryption SDK referensi vektor inisialisasi

Informasi di halaman ini adalah referensi untuk membangun pustaka enkripsi Anda sendiri yang kompatibel dengan file AWS Encryption SDK. Jika Anda tidak membangun pustaka enkripsi kompatibel Anda sendiri, Anda mungkin tidak memerlukan informasi ini.

Untuk menggunakan AWS Encryption SDK dalam salah satu bahasa pemrograman yang didukung, lihatBahasa pemrograman.

Untuk spesifikasi yang mendefinisikan elemen AWS Encryption SDK implementasi yang tepat, lihat AWS Encryption SDK Spesifikasi di GitHub.

AWS Encryption SDK Menyediakan vektor inisialisasi (IVs) yang diperlukan oleh semua suite algoritma yang didukung. SDK menggunakan nomor urut bingkai untuk membangun IV sehingga tidak ada dua frame dalam pesan yang sama yang dapat memiliki IV yang sama.

Setiap 96-bit (12-byte) IV dibangun dari dua array byte besar-endian yang digabungkan dalam urutan sebagai berikut:

- 64 bit: 0 (dicadangkan untuk penggunaan masa depan)
- 32 bit: Nomor urut bingkai. Untuk tag otentikasi header, nilai ini semua nol.

Sebelum pengenalan caching kunci data, AWS Encryption SDK selalu menggunakan kunci data baru untuk mengenkripsi setiap pesan, dan itu menghasilkan semua IVs secara acak. Dihasilkan secara acak aman IVs secara kriptografis karena kunci data tidak pernah digunakan kembali. Ketika SDK memperkenalkan caching kunci data, yang dengan sengaja menggunakan kembali kunci data, kami mengubah cara SDK menghasilkan. IVs

Menggunakan deterministik IVs yang tidak dapat diulang dalam pesan secara signifikan meningkatkan jumlah pemanggilan yang dapat dieksekusi dengan aman di bawah satu kunci data. Selain itu, kunci data yang di-cache selalu menggunakan rangkaian algoritma dengan fungsi derivasi kunci. Menggunakan IV deterministik dengan fungsi derivasi kunci pseudo-acak untuk mendapatkan kunci enkripsi dari kunci data memungkinkan untuk mengenkripsi 2 ^ 32 pesan tanpa melebihi AWS Encryption SDK batas kriptografi.

AWS KMS Rincian teknis keyring hierarkis

Keyring AWS KMS Hierarkis menggunakan kunci data unqiue untuk mengenkripsi setiap pesan dan mengenkripsi setiap kunci data dengan kunci pembungkus unik yang berasal dari kunci cabang aktif. Ini menggunakan derivasi kunci dalam mode counter dengan fungsi pseudorandom dengan HMAC SHA-256 untuk menurunkan kunci pembungkus 32 byte dengan input berikut.

- Garam acak 16 byte
- Kunci cabang aktif
- Nilai yang dikodekan UTF-8 untuk pengenal penyedia kunci "" aws-kms-hierarchy

Keyring Hierarkis menggunakan kunci pembungkus turunan untuk mengenkripsi salinan kunci data teks biasa menggunakan AES-GCM-256 dengan tag otentikasi 16 byte dan input berikut.

- Kunci pembungkus turunan digunakan sebagai kunci sandi AES-GCM
- Kunci data digunakan sebagai pesan AES-GCM
- Vektor inisialisasi acak 12 byte (IV) digunakan sebagai AES-GCM IV
- Data otentikasi tambahan (AAD) yang berisi nilai serial berikut.

Nilai	Panjang dalam byte	Ditafsirkan sebagai
"aws-kms-hierarchy"	17	UTF-8 dikodekan
Pengidentifikasi kunci cabang	Variabel	UTF-8 dikodekan
Versi kunci cabang	16	UTF-8 dikodekan
Konteks enkripsi	Variabel	Pasangan nilai kunci yang dikodekan UTF-8

Riwayat dokumen untuk Panduan AWS Encryption SDK Pengembang

Topik ini menjelaskan pembaruan yang signifikan untuk Panduan Pengembang AWS Encryption SDK .

Topik

Pembaruan terkini

Tabel berikut menjelaskan perubahan signifikan pada dokumentasi ini sejak November 2017. Selain perubahan besar yang tercantum di sini, kami juga sering memperbarui dokumentasi untuk memperbaiki deskripsi dan contoh, serta membahas umpan balik yang Anda kirimkan kepada kami. Untuk diberitahu tentang perubahan signifikan, berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Ketersediaan umum	Menambahkan dokumentasi untuk keyring AWS KMS ECDH dan keyring ECDH mentah.	Juni 17, 2024
AWS Encryption SDK for Java versi 3.x	Mengintegrasikan AWS Encryption SDK for Java dengan perpustakaan penyedia materi. Menambahkan dukungan untuk keyrings dan konteks enkripsi CMM yang diperlukan.	6 Desember 2023
AWS Encryption SDK untuk .NET versi 4.x	Menambahkan dukungan untuk keyring AWS KMS Hierarkis, CMM konteks	12 Oktober 2023

	enkripsi yang diperlukan, dan gantungan kunci RSA asimetris. AWS KMS	
Ketersediaan umum	Memperkenalkan dukungan untuk AWS Encryption SDK untuk .NET.	Mei 17, 2022
Perubahan dokumentasi	Ganti AWS Key Managemen t Service istilah customer master key (CMK) dengan AWS KMS keydan kunci KMS.	Agustus 30, 2021
Ketersediaan umum	Menambahkan dukungan untuk AWS Key Managemen t Service. (AWS KMS) Kunci multi-wilayah. Tombol Multi-Region adalah AWS KMS kunci Wilayah AWS yang berbeda yang dapat digunakan secara bergantian karena memiliki ID kunci dan bahan kunci yang sama.	8 Juni 2021
Ketersediaan umum	Ditambahkan dan diperbarui dokumentasi tentang proses dekripsi pesan ditingkatkan.	11 Mei 2021
Ketersediaan umum	Dokumentasi yang ditambahk an dan diperbarui untuk rilis ketersediaan umum AWS Enkripsi CLI versi 1.8. x untuk mengganti AWS Enkripsi CLI versi 1.7. x, dan AWS Enkripsi CLI 2.1. x untuk mengganti AWS Enkripsi CLI 2.0. x.	27 Oktober 2020

Ketersediaan umum	Ditambahkan dan diperbaru i dokumentasi untuk rilis ketersediaan umum AWS Encryption SDK versi 1.7. x dan 2.0. x, termasuk panduan praktik terbaik, panduan migrasi, konsep yang diperbarui, topik bahasa pemrograman yang diperbarui, referensi suite algoritme yang diperbarui, referensi format pesan yang diperbarui, dan contoh format pesan baru.	24 September 2020
Ketersediaan umum	Ditambahkan dan diperbaru i dokumentasi untuk rilis ketersediaan umum dari AWS Encryption SDK for JavaScript.	1 Oktober 2019
Rilis pratinjau	Dokumentasi yang ditambahk an dan diperbarui dari rilis beta publik dari AWS Encryption SDK for JavaScript.	21 Juni 2019
Ketersediaan umum	Ditambahkan dan diperbaru i dokumentasi untuk rilis ketersediaan umum dari AWS Encryption SDK for C.	16 Mei 2019
Rilis pratinjau	Ditambahkan dokumentasi dari rilis pratinjau dari AWS Encryption SDK for C.	5 Februari 2019
Rilis baru	Menambahkan dokumenta si antarmuka baris perintah untuk file AWS Encryption SDK.	20 November 2017

Pembaruan lebih awal

Tabel berikut menjelaskan perubahan signifikan pada Panduan AWS Encryption SDK Pengembang sebelum November 2017.

Ubah	Deskripsi	Date
Rilis baru	Menambahkan Caching kunci data chapter untuk fitur baru. Menambahkan the section called “Referensi vektor inisialisasi” topik yang menjelaskan bahwa SDK berubah dari menghasilkan acak menjadi IVs membangun deterministik. IVs Menambahkan the section called “Konsep” topik untuk menjelaskan konsep, termasuk manajer bahan kriptografi baru.	Juli 31, 2017
Perbarui	Memperluas Referensi format pesan dokumentasi ke AWS Encryption SDK referensi bagian baru. Menambahkan bagian tentang AWS Encryption SDK Suite algoritma yang didukung.	Maret 21, 2017
Rilis baru	AWS Encryption SDK Sekarang mendukung bahasa Python pemrograman, selainJava.	Maret 21, 2017

Ubah	Deskripsi	Date
Rilis awal	Rilis awal dokumentasi AWS Encryption SDK dan ini.	Maret 22, 2016

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.