Guía del usuario de

AWS Criptografía de pagos

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Criptografía de pagos: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas registradas y la imagen comercial de Amazon no se pueden utilizar en ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es la criptografía de AWS pagos? 1
Conceptos 2
Terminología del sector 4
Tipos de claves comunes 4
Otros términos 8
Servicios relacionados 13
Para obtener más información 14
Puntos de conexión 14
Puntos de conexión del plano de control 14
Puntos de conexión del plano de datos 17
Introducción 21
Requisitos previos 21
Paso 1: crear una clave 22
Paso 2: Genere un valor con la clave CVV2 23
Paso 3: verificar el valor generado en el paso 2 23
Paso 4: realizar una prueba negativa 24
Paso 5: eliminación (opcional) 24
Administración de claves 26
Crear claves 26
Creación de una clave de derivación base TDES de 3 teclas 27
Crear una clave TDES de 2 teclas para CVV/CVV2 29
Crear una clave HMAC 30
Crear una clave AES-256 31
Creación de una clave de cifrado PIN (PEK) 32
Crear una clave asimétrica (RSA) 33
Creación de una clave de valor de verificación de PIN (PVV) 34
Crear una clave ECC asimétrica 35
Enumerar las claves 36
Habilitación y desactivación de claves de 38
Iniciar el uso de claves 38
Detener el uso de claves 40
Claves de replicación 42
Ventajas de la replicación de claves Multi-Region 42
Cómo funciona la replicación de Multi-Region claves 42

Limitaciones y consideraciones 42
Habilitar Multi-Region la replicación de claves 43
Deshabilitar Multi-Region la replicación de claves 46
Consideraciones de seguridad 47
Prácticas recomendadas 47
Precios 47
Eliminación de claves de 47
Acerca del período de espera 48
Importación y exportación de claves 52
Importar claves 54
Exportar claves 80
Temas avanzados 103
Uso de alias 115
Acerca de los alias 116
Usar alias en las aplicaciones 119
API relacionadas 120
Obtener claves 120
Haga que el público key/certificate se asocie a un key pair 122
Etiquetado de claves 123
Acerca de las etiquetas en la criptografía de pagos AWS 123
Visualización de etiquetas clave en la consola 125
Administración de etiquetas de clave con operaciones de la API 125
Control del acceso a las etiquetas 128
Uso de etiquetas para controlar el acceso a las claves 132
Comprender los atributos de las claves 136
Claves simétricas 136
Claves asimétricas 138
Operaciones de datos 140
Cifrar, descifrar y volver a cifrar datos 140
Cifrar datos 141
Descifrado de datos 147
Generación y verificación de datos de tarjetas 151
Generar datos de tarjetas 152
Comprobación de datos de tarjetas 153
Generar, traducir y verificar los datos del PIN 155
Traducir datos PIN 156

Generar datos PIN 158
Comprobación de datos PIN 162
Verificar el criptograma de solicitud de autenticación (ARQC) 166
Creación de datos de transacciones 167
Relleno de datos de transacciones 167
Ejemplos 169
Generar y verificar MAC 170
Generar MAC 172
Verificar MAC 176
Tipos de clave para operaciones de datos específicas 178
GenerateCardData 179
VerifyCardData 180
GeneratePinData (para VISA/ABA esquemas) 181
GeneratePinData (para) IBM3624 182
VerifyPinData (para esquemas) VISA/ABA 183
VerifyPinData (para) IBM3624 184
Descifrado de datos 185
Cifrado de datos 186
Traducir datos PIN 187
Generar/verificar el MAC 188
GenerateMacEmvPinChange 189
VerifyAuthRequestCryptogram 191
Clave de Importación/Exportación 191
Tipos de claves sin utilizar 192
Casos de uso comunes 193
Emisores y procesadores de emisores 193
Funciones generales 193
Funciones específicas de la red 213
Facilitadores de adquisiciones y pagos 239
Uso de claves dinámicas 240
Características específicas de la región 243
AS2805 243
Intercambio de clave inicial (KEK) 245
Validación de la KEK 247
Creación y transmisión de claves de trabajo 250
Exportación de claves de trabajo 252

Traducción de pines 253
Generación y validación de Mac 254
Seguridad 255
Protección de datos 256
Rotación del material de claves 257
Cifrado de datos 257
Cifrado en reposo 257
Cifrado en tránsito 258
Privacidad del tráfico entre redes 258
Resiliencia 259
Aislamiento regional 259
Multi-tenant diseño 260
Seguridad de la infraestructura 261
Aislamiento de hosts físicos 261
Utilice Amazon VPC y AWS PrivateLink 261
Consideraciones sobre los puntos AWS finales de VPC de criptografía de pagos 262
Creación de un punto final de VPC para AWS criptografía de pagos 263
Conectar con un punto de conexión de VPC 264
Control del acceso a un punto de conexión de VPC 265
Utilizar un punto de conexión de VPC en una declaración de política 269
Registro de su punto de conexión de VPC 272
TLS híbrido postcuántico 275
Acerca del cifrado TLS postcuántico 276
Acerca de PQC 276
Modo de uso 277
Prácticas recomendadas de seguridad 280
Validación de conformidad 283
Conformidad del servicio 283
Cumplimiento de los PIN 284
Temas comunes 284
Alcance de la evaluación 287
Operaciones de procesamiento de transacciones 289
Conformidad con P2PE 295
Identity and Access Management 296
Público 296
Autenticación con identidades 297

Cuenta de AWS usuario root 297
Usuarios y grupos de IAM 297
Roles de IAM 297
Administración del acceso con políticas 298
Identity-based políticas 298
Resource-based políticas 298
Listas de control de acceso (ACL) 299
Otros tipos de políticas 299
Varios tipos de políticas 299
Cómo funciona la criptografía de AWS pagos con IAM 300
AWS Políticas de criptografía de pagos Identity-based 300
Autorización basada en etiquetas de criptografía de pago AWS 302
Identity-based ejemplos de políticas 302
Prácticas recomendadas relativas a políticas 303
Uso de la consola 304
Permitir a los usuarios consultar sus propios permisos 305
Posibilidad de acceder a todos los aspectos de la criptografía de pagos AWS 306
Posibilidad de llamar a las API mediante claves específicas 306
Capacidad para denegar específicamente un recurso 307
Resource-based políticas 308
Consideraciones 309
Administrar las políticas basadas en los recursos 310
Resource-based ejemplos de políticas 312
Multi-party aprobación 313
Descripción general de 314
Operaciones protegidas 314
Requisitos previos 315
Activación y desactivación de la MPA 315
Introducción 316
Ejemplo: importe un certificado raíz con la MPA habilitada 316
AWS CloudTrail registro de eventos de MPA 318
Comprobar el estado de las solicitudes y gestionar los errores 320
Resolución de problemas 322
Monitorización 323
CloudTrail registros 324
AWS Información sobre criptografía de pagos en CloudTrail 324

Controle los eventos del plano en CloudTrail 325
Eventos de datos en CloudTrail 325
Comprensión AWS de las entradas de los archivos de registro del plano de control de criptografía de pagos 327
Descripción de las entradas de los archivos de registro del plano de datos de criptografía de AWS pagos 330
Detalles criptográficos 333
Objetivos de diseño 334
Principios básicos 335
Primitivas criptográficas 335
Entropía y generación de números aleatorios 336
Operaciones de clave simétrica 336
Operaciones con claves asimétricas 336
Almacenamiento de claves 337
Importación de claves simétricas 337
Importación de claves con claves asimétricas 337
Exportación de claves 338
Protocolo de clave única derivada por transacción (DUKPT) 338
Jerarquía de claves 338
Operaciones internas 342
Protección HSM 342
Administración general de claves 345
Gestión de las claves de los clientes 349
Seguridad de las comunicaciones 351
Registro y supervisión 352
Operaciones de clientes 352
Generación de claves 353
Importación de claves 353
Exportación de claves 354
Eliminación de claves de 355
Rotar claves de 355
Cuotas 356
Historial de revisión 358
..... ccclx

¿Qué es la criptografía de AWS pagos?

AWS La criptografía de pagos es un AWS servicio gestionado que proporciona acceso a las funciones criptográficas y a la gestión de claves que se utilizan en el procesamiento de pagos de conformidad con los estándares del sector de las tarjetas de pago (PCI), sin necesidad de adquirir instancias de HSM de pago dedicadas. AWS La criptografía de pagos ofrece a los clientes que realizan funciones de pago, como los adquirentes, los facilitadores de pagos, las redes, los conmutadores, los procesadores y los bancos, la posibilidad de acercar sus operaciones criptográficas de pago a las aplicaciones en la nube y minimizar la dependencia de los centros de datos auxiliares o las instalaciones de colocación que contienen pagos dedicados HSMs.

El servicio está diseñado para cumplir con las normas aplicables de la industria, incluidas PCI PIN, PCI P2PE y PCI DSS, y aprovecha el hardware que cuenta con la certificación PCI PTS HSM V3 y FIPS 140-2 de nivel 3. Está diseñada para soportar una baja latencia y altos niveles de tiempo de actividad y resiliencia. AWS La criptografía de pagos es totalmente elástica y elimina muchos de los requisitos operativos de las instalaciones locales HSMs, como la necesidad de aprovisionar hardware, gestionar de forma segura el material clave y mantener las copias de seguridad de emergencia en instalaciones seguras. AWS La criptografía de pagos también le ofrece la opción de compartir las claves con sus socios de forma electrónica, lo que elimina la necesidad de compartir componentes de texto transparente en papel.

Puede usar la API del plano de control de AWS Payment Cryptography para crear y administrar claves.

Puede usar la API del plano de datos de AWS Payment Cryptography para usar claves de cifrado para el procesamiento de transacciones relacionadas con los pagos y las operaciones criptográficas asociadas.

AWS La criptografía de pagos ofrece funciones importantes que puede utilizar para gestionar sus claves:

- Cree y gestione claves de criptografía de AWS pagos simétricas y asimétricas, incluidas las claves TDES, AES y RSA, y especifique su propósito, por ejemplo, para la generación de CVV o la obtención de claves DUKPT.
- Guarde automáticamente sus claves de criptografía AWS de pagos de forma segura, protegidas por módulos de seguridad de hardware (), al tiempo que establece la separación de claves entre los casos de uso. HSMs

- Cree, elimine, enumere y actualice los alias, que son «nombres descriptivos» que se pueden usar para acceder o controlar el acceso a sus claves de criptografía de AWS pagos.
- Etiquete sus claves AWS de criptografía de pagos para identificarlas, agruparlas, automatizarlas, controlar el acceso y hacer un seguimiento de los costes.
- Importe y exporte claves simétricas entre AWS Payment Cryptography y su HSM (o terceros) mediante claves de cifrado de claves (KEK) según la norma TR-31 (especificación de bloques de claves de intercambio seguro de claves interoperable).
- Importe y exporte claves de cifrado de claves simétricas (KEK) entre AWS Payment Cryptography y otros sistemas mediante pares de claves asimétricas y, a continuación, utilice medios electrónicos como el TR-34 (método de distribución de claves simétricas mediante técnicas asimétricas).

Puede utilizar sus claves de criptografía de AWS pago en operaciones criptográficas, como:

- Cifre, descifre y vuelva a cifrar los datos con claves de criptografía de pagos simétricas o asimétricas. AWS
- Traducir de forma segura los datos sensibles (como los PIN de los titulares de tarjetas) entre claves de cifrado sin exponer el texto en claro, de acuerdo con las normas PCI sobre PIN.
- Genere o valide los datos del titular de la tarjeta, como el CVV o el ARQC. CVV2
- Generar y validar los pines del titular de la tarjeta.
- Generar o validar las firmas MAC.

Conceptos

Conozca los términos y conceptos básicos que se utilizan en la criptografía de AWS pagos y cómo puede utilizarlos para proteger sus datos.

Alias

> Un nombre fácil de usar que está asociado a una clave de criptografía AWS de pagos. El alias se puede usar indistintamente con la clave ARN en muchas de las operaciones de la API de criptografía de AWS pagos. Los alias permiten rotar o cambiar las claves sin que ello afecte al código de su aplicación. El nombre de alias es una cadena de hasta 256 caracteres. Identifica de forma exclusiva una clave de criptografía AWS de pagos asociada dentro de una cuenta y una región. En la criptografía de AWS pagos, los nombres de alias siempre comienzan por. `alias/`

El formato de un nombre de alias es el siguiente:

```
alias/<alias-name>
```

Por ejemplo:

```
alias/sampleAlias2
```

ARN de clave

El ARN de la clave es el nombre de recurso de Amazon (ARN) de una entrada de clave en AWS Payment Cryptography. Se trata de un identificador único y totalmente cualificado para la clave de criptografía AWS de pagos. Un ARN clave incluye una región Cuenta de AWS, y un ID generado aleatoriamente. El ARN no está relacionado ni se deriva del material de la clave. Como se asignan automáticamente durante las operaciones de creación o importación, estos valores no son idempotentes. Si se importa la misma clave varias veces, se obtendrá una clave múltiple ARNs con su propio ciclo de vida.

El formato de un ARN de clave es el siguiente:

```
arn:<partition>:payment-cryptography:<region>:<account-id>:alias/<alias-name>
```

A continuación, se muestra un ARN de clave de ejemplo.

```
arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h
```

Identificador de clave

Un identificador de clave es una referencia a una clave y una (o más) de ellas son entradas típicas de las operaciones de criptografía de AWS pagos. Los identificadores de clave válidos pueden ser una clave o un alias de clave.

AWS Claves de criptografía de pago

AWS Las claves de criptografía de pago (claves) se utilizan para todas las funciones criptográficas. Las claves se generan directamente mediante el comando crear clave o se añaden al sistema al llamar a la importación de claves. El origen de una clave se puede determinar revisando el atributo. KeyOrigin AWS La criptografía de pagos también admite claves derivadas o intermedias que se utilizan durante las operaciones criptográficas, como las que utiliza DUKPT.

Estas claves tienen atributos inmutables y mutables definidos en el momento de su creación. Los atributos, como el algoritmo, la longitud y el uso, se definen en el momento de la creación y no se pueden cambiar. Otros, como la fecha de entrada en vigor o la fecha de caducidad, se pueden modificar. Consulte la referencia de la API AWS de criptografía de pagos para obtener una lista completa de los atributos de las claves de criptografía de AWS pagos.

AWS Las claves de criptografía de pago tienen tipos de claves, definidos principalmente en la norma ANSI X9 TR 31, que restringen su uso a los fines previstos, tal como se especifica en el requisito 19 del PCI PIN v3.1.

Los atributos se vinculan a las claves mediante bloques de claves cuando se almacenan, se comparten con otras cuentas o se exportan, tal y como se especifica en el requisito 18-3 de PCI PIN v3.1.

Las claves se identifican en la plataforma de criptografía de AWS pagos mediante un valor único conocido como clave Amazon Resource Name (ARN).

> **Note**
>
> ARNLa clave se genera cuando se crea o importa inicialmente una clave al servicio de criptografía AWS de pagos. Por lo tanto, si añade el mismo material clave varias veces utilizando la funcionalidad de importación de claves, el mismo material clave se encontrará bajo varias claves ARNS pero cada una con un ciclo de vida clave diferente.

Terminología del sector

Temas

- Tipos de claves comunes
- Otros términos

Tipos de claves comunes

AWS Clave de criptografía de pago

Una clave AWS de criptografía de pago existe en una sola. Región de AWS Consiste en metadatos y material clave almacenados en el Servicio de Criptografía AWS de Pagos. Una clave

puede importarse de una fuente externa como un bloque de TR-31 claves o generarse mediante el Servicio de criptografía AWS de pagos.

AWK

Una clave de trabajo del adquirente (AWK) es una clave que se utiliza normalmente para intercambiar datos entre un acquirer/acquirer procesador y una red (como Visa o Mastercard). Históricamente, AWK utiliza el 3DES para el cifrado y se representa como TR31_P0_PIN_ENCRYPTION_KEY.

BDK

Una clave de derivación base (BDK) es una clave funcional que se utiliza para derivar claves posteriores y se utiliza normalmente como parte del proceso PCI PIN y PCI P2PE DUKPT. Se denomina TR31_B0_BASE_DERIVATION_KEY.

CMK

Una clave maestra de tarjeta (CMK) es una o más claves específicas de una tarjeta que normalmente se derivan de una clave maestra del emisor, un PAN y una PSN y, por lo general, son claves 3DES. Estas claves se almacenan en el chip EMV durante la personalización. Entre los ejemplos de CMK se incluyen las teclas AC, SMI y SMC.

CMK-AC

Una clave de criptograma de aplicación (AC) se utiliza como parte de las transacciones EMV para generar el criptograma de la transacción y es un tipo de clave maestra de tarjeta.

CMK-SMI

Una clave de integridad de mensajería segura (SMI) se utiliza como parte de EMV para verificar la integridad de las cargas útiles enviadas a la tarjeta mediante MAC, como los scripts de actualización de PIN. Es un tipo de clave maestra de la tarjeta.

CMK-SMC

Como parte del EMV, se utiliza una clave de confidencialidad segura de la mensajería (SMC) para cifrar los datos enviados a la tarjeta, como las actualizaciones del PIN. Es un tipo de clave maestra de la tarjeta.

CVK

Una clave de verificación de tarjeta (CVK) es una clave que se utiliza para generar valores CVV, CVV2 y similares mediante un algoritmo definido, así como para validar una entrada. Se denomina TR31_C0_CARD_VERIFICATION_KEY.

IMK

Una clave maestra del emisor (IMK) es una clave maestra que se utiliza como parte de la personalización de la tarjeta con chip EMV. Normalmente, habrá 3 IMK: una para las claves AC (criptograma), SMI (clave maestra de script para) y SMC (clave maestra de script para integrity/signature). confidentiality/encryption

IK

Una clave inicial (IK) es la primera clave que se utiliza en el proceso DUKPT y se deriva de la clave de derivación básica (BDK). No se procesa ninguna transacción en esta clave, pero se usa para derivar claves futuras que se usarán para las transacciones. El método de derivación para crear una IK se definió en. X9.24-1:2017 Cuando se utiliza un BDK TDES, X9.24-1:2009 es el estándar aplicable y el IK se sustituye por la clave de cifrado con PIN inicial (IPEK).

IPEK

Una clave de cifrado de PIN inicial (IPEK) es la clave inicial que se utiliza en el proceso DUKPT y se deriva de la clave de derivación básica (BDK). No se procesa ninguna transacción en esta clave, pero se usa para derivar claves futuras que se usarán para las transacciones. IPEK es un nombre inapropiado, ya que esta clave también se puede utilizar para derivar claves de cifrado de datos y de Mac. El método de derivación para crear un IPEK se definió en. X9.24-1:2009 Cuando se utiliza un BDK de AES, X9.24-1:2017 es el estándar aplicable y el IPEK se sustituye por la clave inicial (IK).

IWK

Una clave de trabajo del emisor (IWK) es una clave que se utiliza normalmente para intercambiar datos entre un issuer/issuer procesador y una red (como Visa o Mastercard). Históricamente, IWK utiliza el 3DES para el cifrado y se representa como TR31_P0_PIN_ENCRYPTION_KEY.

KBPK

Una clave de cifrado de bloques de claves (KBPK) es un tipo de clave simétrica que se utiliza para proteger los bloques de claves y, por lo tanto, otras claves. wrap/encrypt Una KBPK es similar a una KEK, pero una KEK protege directamente el material de la clave, mientras que en TR-31 esquemas similares, la KBPK solo protege indirectamente la clave de trabajo. Cuando se

utiliza TR-31, TR31_K1_KEY_BLOCK_PROTECTION_KEY es el tipo de clave correcto, aunque TR31_K0_KEY_ENCRYPTION_KEY se admite indistintamente con fines históricos.

KEK

Una clave de cifrado clave (KEK) es una clave que se utiliza para cifrar otras claves, ya sea para su transmisión o almacenamiento. Las claves destinadas a proteger otras claves suelen tener el valor TR31_K0_KEY_ENCRYPTION_KEY según el estándar. KeyUsage *TR-31*

PEK

Una clave de cifrado de PIN (PEK) es un tipo de clave funcional que se utiliza para cifrar los PIN, ya sea para su almacenamiento o transmisión entre dos partes. IWK y AWK son dos ejemplos de usos específicos de las claves de cifrado de PIN. Estas claves se representan como TR31_P0_PIN_ENCRYPTION_KEY.

PGK

PGK (clave de generación de PIN) es otro nombre para una clave de verificación de PIN. En realidad, no se usa para generar pines (que por defecto son números criptográficamente aleatorios), sino que se usa para generar valores de verificación como el PVV.

PRK

La clave de la región principal es la fuente de replicación autorizada de una clave de criptografía de pago determinada para la que se ha activado la replicación. PRK es una referencia a la función clave de la criptografía de pagos de origen en una Multi-Region configuración de replicación de claves. Cuando la replicación está habilitada en una clave de criptografía de pago, se denomina PRK para esa configuración de replicación de claves específica.

PVK

Una clave de verificación de PIN (PVK) es un tipo de clave de trabajo que se utiliza para generar valores de verificación de PIN, como la PVV. Los dos tipos más comunes son el TR31_V1_IBM3624_PIN_VERIFICATION_KEY, que se usa para generar valores de compensación del IBM3624, y el TR31_V2_VISA_PIN_VERIFICATION_KEY, que se usa para los valores de verificación. Visa/ABA También se conoce como clave de generación de pines.

KRK

Las claves de región de réplica son el material clave y los metadatos replicados que se copian de forma segura desde la PRK a una réplica configurada. Región de AWS Una RRK es una réplica de solo lectura de una clave de criptografía de pago. La RRK es una referencia, el papel que desempeña una clave específica en una configuración de replicación de Multi-Region claves.

Todos los cambios clave en los metadatos, incluida la configuración de replicación, deben aplicarse a la PRK.

Otros términos

ARQC

El criptograma de solicitud de autorización (ARQC) es un criptograma generado en el momento de la transacción mediante una tarjeta con chip estándar EMV (o una implementación sin contacto equivalente). Por lo general, un ARQC se genera mediante una tarjeta con chip y se envía al emisor o a su agente para su verificación en el momento de la transacción.

CVV

El valor de verificación de una tarjeta es un valor secreto estático que, tradicionalmente, estaba incrustado en una banda magnética y se utilizaba para validar la autenticidad de una transacción. El algoritmo también se utiliza para otros fines, como iCVV, CAVV, CVV2. Es posible que no esté integrado de esta manera para otros casos de uso.

CVV2

El valor de verificación de una tarjeta 2 es un valor secreto estático que tradicionalmente se imprimía en el anverso (o reverso) de una tarjeta de pago y que se utiliza para verificar la autenticidad de los pagos con tarjetas no presentes (por ejemplo, por teléfono o en línea). Utiliza el mismo algoritmo que el CVV, pero el código de servicio está establecido en 000.

iCVV

iCVV es un CVV2-like valor, pero está integrado con los datos equivalentes a track2 en una tarjeta EMV (chip). Este valor se calcula con un código de servicio 999 y es diferente al utilizado CVV1/CVV2 para evitar que la información robada se utilice para crear nuevas credenciales de pago de otro tipo. Por ejemplo, si se obtuvieron datos de transacciones con chips, no es posible utilizarlos para generar una banda magnética (CVV1) ni para realizar compras en línea (CVV2).

Utiliza una clave ???

DUKPT

La clave única derivada por transacción (DUKPT) es un estándar de administración de claves que se suele utilizar para definir el uso de claves de cifrado físicas de un solo uso. POS/POI Históricamente, DUKPT utiliza el 3DES para el cifrado. El estándar industrial para el DUKPT se define en el ANSI. X9.24-3-2017

ECC

El ECC (criptografía de curva elíptica) es un sistema de criptografía de clave pública que utiliza las matemáticas de las curvas elípticas para crear claves de cifrado. El ECC proporciona el mismo nivel de seguridad que los métodos tradicionales, como el RSA, pero con longitudes de clave mucho más cortas, lo que proporciona una seguridad equivalente de una manera más eficiente. Esto es especialmente relevante para los casos de uso en los que RSA no es una solución práctica (longitud de clave RSA superior a 4096 bits). AWS La criptografía de pagos admite curvas definidas por el NIST para su uso en las operaciones del ECDH.

ECDH

El ECDH (curva elíptica Diffie-Hellman) es un protocolo de acuerdo clave que permite a dos partes establecer un secreto compartido (como un KEK o un PEK). En el ECDH, las Partes A y B tienen sus propios pares de claves público-privadas e intercambian claves públicas entre sí (en forma de certificados de criptografía de AWS pago), así como metadatos de derivación de claves (método de derivación, tipo de hash e información compartida). Ambas partes multiplican su clave privada por la clave pública de la otra y, gracias a las propiedades de la curva elíptica, ambas partes pueden derivar (generar) la clave resultante.

EMV

EMV (originalmente Europay, Mastercard y Visa) es un organismo técnico que trabaja con las partes interesadas en los pagos para crear estándares y tecnologías de pago interoperables. Un ejemplo de norma es el de chip/contactless las tarjetas y los terminales de pago con los que interactúan, incluida la criptografía utilizada. La derivación de claves EMV se refiere a los métodos que permiten generar claves únicas para cada tarjeta de pago a partir de un conjunto inicial de claves, como una `IMK`

HSM

Un módulo de seguridad de hardware (HSM) es un dispositivo físico que protege las operaciones criptográficas (por ejemplo, el cifrado, el descifrado y las firmas digitales), así como las claves subyacentes que se utilizan para estas operaciones.

KCAAS

Un custodio de claves como servicio (KCAAS) proporciona una variedad de servicios relacionados con la administración de claves. En el caso de las claves de pago, normalmente pueden convertir los componentes clave en papel en formularios electrónicos compatibles con la criptografía de AWS pago o convertir las claves protegidas electrónicamente en componentes en papel que podrían necesitar algunos proveedores. También pueden ofrecer servicios de

custodia de llaves para las llaves cuya pérdida sería perjudicial para sus operaciones en curso. Los proveedores de KCAAS pueden ayudar a los clientes a reducir la carga operativa que supone gestionar el material clave fuera de un servicio seguro, como la criptografía de AWS pagos, de forma que cumplan con las normas PCI DSS, PCI PIN y PCI P2PE. AWS La criptografía de pagos ofrece Intercambio de claves físicas una capacidad KCAAS integrada para convertir componentes clave en papel a formato electrónico.

KCV

El valor de comprobación de claves (KCV) se refiere a una variedad de métodos de suma de comprobación que se utilizan principalmente para comparar claves entre sí sin tener acceso al material de las claves propiamente dichas. Los KCV también se han utilizado para validar la integridad (especialmente cuando se intercambian claves), aunque esta función ahora se incluye como parte de los formatos de bloques de claves, como TR-31. En el caso de las claves TDES, el KCV se calcula cifrando 8 bytes, cada uno con un valor igual a cero, con la clave que hay que comprobar y reteniendo los 3 bytes más importantes del resultado cifrado. En el caso de las claves AES, el KCV se calcula mediante un algoritmo CMAC en el que los datos de entrada son 16 bytes de cero y se retienen los 3 bytes de orden superior del resultado cifrado.

KDH

Un host de distribución de claves (KDH) es un dispositivo o sistema que envía claves en un proceso de intercambio de claves, por ejemplo. TR-34 Cuando se envían claves desde AWS Payment Cryptography, se considera el KDH.

KIF

Un servicio de inyección de claves (KIF) es un servicio seguro que se utiliza para inicializar los terminales de pago e incluso cargarlos con claves de cifrado.

KRD

Un dispositivo receptor de claves (KRD) es un dispositivo que recibe claves en un proceso de intercambio de claves, como. TR-34 Al enviar claves a la criptografía de AWS pagos, se considera el KRD.

KSN

Un número de serie clave (KSN) es un valor que se utiliza como entrada en DUKPT encryption/decryption para crear claves de cifrado únicas por transacción. Por lo general, el KSN consta de un identificador BDK, un identificador de terminal semi-exclusivo y un contador de transacciones que se incrementa con cada transición procesada en un terminal de pago determinado. Por

ejemplo X9.24, en el caso del TDES, el KSN de 10 bytes suele constar de 24 bits para el ID del conjunto de claves, 19 bits para el ID del terminal y 21 bits para el contador de transacciones, aunque el límite entre el ID del conjunto de claves y el ID del terminal no afecta a la función de la criptografía de pagos. AWS En el caso del AES, el KSN de 12 bytes suele constar de 32 bits para el ID del BDK, 32 bits para el identificador de derivación (ID) y 32 bits para el contador de transacciones.

mPoC

El mPoC (punto de venta móvil con hardware comercial) es un estándar PCI que aborda los requisitos de seguridad de las soluciones que permiten a los comerciantes aceptar PIN de los titulares de tarjetas o pagos sin contacto mediante un teléfono inteligente u otros dispositivos móviles comerciales listos para usar (COTS).

PAN

El número de cuenta principal (PAN) es un identificador único para una cuenta, como una tarjeta de crédito o débito. Suele tener entre 13 y 19 dígitos. Los primeros 6 a 8 dígitos identifican la red y el banco emisor.

Bloqueo de PIN

Un bloque de datos que contiene un PIN durante el procesamiento o la transmisión, así como otros elementos de datos. Los formatos de bloque de PIN estandarizan el contenido del bloque de PIN y la forma en que se puede procesar para recuperar el PIN. La mayoría de los bloques de PIN están compuestos por el PIN, la longitud del PIN y, con frecuencia, contienen parte o todo el PAN. AWS La criptografía de pagos es compatible con los formatos ISO 9564-1 0, 1, 3 y 4. El formato 4 es obligatorio para las claves AES. Al verificar o traducir los PIN, es necesario especificar el bloque de PIN de los datos entrantes o salientes.

POI

El punto de interacción (POI), que también se utiliza con frecuencia de forma anónima con el punto de venta (POS), es el dispositivo de hardware con el que el titular de la tarjeta interactúa para presentar su credencial de pago. Un ejemplo de POI es la terminal física de un establecimiento comercial. Para ver la lista de terminales POI PCI PTS certificados, consulte el sitio web de PCI.

PSN

El número de secuencia PAN (PSN) es un valor numérico que se utiliza para diferenciar varias tarjetas emitidas con el mismo PAN.

Clave pública

Cuando se utilizan cifrados asimétricos (RSA, ECC), la clave pública es el componente público de un par de claves público-privadas. La clave pública se puede compartir y distribuir a entidades que necesitan cifrar datos para el propietario del par de claves público-privado. Para las operaciones de firma digital, la clave pública se utiliza a fin de verificar la firma.

Clave privada

Cuando se utilizan cifrados asimétricos (RSA, ECC), la clave privada es el componente privado de un par de claves público-privadas. La clave privada se utiliza para descifrar los datos o crear firmas digitales. Al igual que las claves simétricas de criptografía AWS de pagos, los HSM crean las claves privadas de forma segura. Solo se descifran en la memoria volátil del HSM y únicamente durante el tiempo necesario para procesar su solicitud criptográfica.

PVV

Un valor de verificación de PIN (PVV) es un tipo de salida criptográfica que se puede utilizar para verificar un PIN sin almacenar el pin real. Aunque es un término genérico, en el contexto de la criptografía de AWS pagos, PVV se refiere al método PVV de Visa o ABA. Este PVV es un número de cuatro dígitos cuyas entradas son el número de la tarjeta, el número de secuencia panorámica, la propia bandeja y una clave de verificación del PIN. Durante la fase de validación, AWS Payment Cryptography recrea internamente el PVV utilizando los datos de la transacción y lo compara de nuevo con el valor almacenado por el AWS cliente de Payment Cryptography. En este sentido, es conceptualmente similar a un hash criptográfico o MAC.

RSA Wrap/Unwrap

La envoltura RSA utiliza una clave asimétrica para envolver una clave simétrica (como una clave TDES) para su transmisión a otro sistema. Solo el sistema con la clave privada coincidente puede descifrar la carga útil y cargar la clave simétrica. Por el contrario, RSA unwrap descifrará de forma segura una clave cifrada con RSA y, a continuación, la cargará en la criptografía de pagos. AWS El empaquetado RSA es un método de bajo nivel para intercambiar claves y no transmite las claves en formato de bloque de claves ni utiliza la firma de carga útil por parte de la parte que las envía. Se deben considerar controles alternativos para determinar la procedencia y comprobar que los atributos clave no están mutados.

TR-34 también utiliza RSA internamente, pero es un formato independiente y no es interoperable.

TR-31

TR-31 (definido formalmente como ANSI X9 TR 31) es un formato de bloques clave definido por el Instituto Nacional de Normalización de los Estados Unidos (ANSI) para permitir la definición de los atributos clave en la misma estructura de datos que los propios datos clave. El formato de bloque de TR-31 teclas define un conjunto de atributos clave que están vinculados a la clave para que se mantengan unidos. AWS La criptografía de pagos utiliza términos TR-31 estandarizados siempre que es posible para garantizar una separación y un propósito adecuados de las claves. TR-31 ha sido sustituida por el ANSI. X9.143-2022

TR-34

TR-34 es una implementación del ANSI X9.24-2 que describe un protocolo para distribuir de forma segura claves simétricas (como 3DES y AES) mediante técnicas asimétricas (como RSA). AWS La criptografía de pagos utiliza TR-34 métodos que permiten la importación y exportación seguras de claves.

X9.143

X9.143 es un formato de bloque de claves definido por el Instituto Nacional de Normalización de los Estados Unidos (ANSI) para proteger una clave y sus atributos en la misma estructura de datos. El formato de bloque de claves define un conjunto de atributos clave que están vinculados a la clave para que se mantengan unidos. AWS La criptografía de pagos utiliza términos X9.143 estandarizados siempre que es posible para garantizar una separación y un propósito adecuados de las claves. X9.143 sustituye a la TR-31propuesta anterior, aunque en la mayoría de los casos son compatibles con versiones anteriores y posteriores y los términos suelen utilizarse indistintamente.

Servicios relacionados

AWS Key Management Service

AWS El Servicio de administración de claves (AWS KMS) es un servicio administrado que le facilita la creación y el control de las claves criptográficas que se utilizan para proteger sus datos. AWS KMS utiliza módulos de seguridad de hardware (HSMs) para proteger y validar las claves de AWS KMS.

AWS CloudHSM

AWS CloudHSM proporciona a los clientes instancias de HSM dedicadas de uso general en la AWS nube. AWS CloudHSM puede proporcionar una variedad de funciones criptográficas, como la creación de claves, la firma de datos o el cifrado y descifrado de datos.

Para obtener más información

- Para obtener más información sobre los términos y conceptos utilizados en la criptografía de AWS pagos, consulte AWS Conceptos de criptografía de pagos.
- Para obtener información sobre la API del plano de control de criptografía de AWS pagos, consulte la referencia de la API del plano de control AWS de criptografía de pagos.
- Para obtener información sobre la API del plano de datos de criptografía de AWS pagos, consulte la referencia de la API del plano de datos AWS de criptografía de pagos.
- Para obtener información técnica detallada sobre cómo la criptografía de AWS pagos utiliza la criptografía y protege las claves de criptografía de AWS pagos, consulte Detalles criptográficos.

Puntos finales para AWS Payment Cryptography

Para conectarse mediante programación AWS Payment Cryptography, utilice un punto final, la URL del punto de entrada al servicio. AWS Los SDK y las herramientas de línea de comandos utilizan automáticamente el punto final predeterminado para el servicio en Región de AWS función del contexto regional de la solicitud, por lo que normalmente no es necesario establecer estos valores de forma explícita. Cuando sea necesario, puedes especificar un punto final diferente para tus solicitudes de API.

Puntos de conexión del plano de control

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (Ohio)	us-east-2	controlplane.payment-cryptography.us-east-2.amazonaws.com	HTTPS HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
		controlplane.payment-cryptography.us-east-2.api.aws	
Este de EE. UU. (Norte de Virginia)	us-east-1	controlplane.payment-cryptography.us-east-1.amazonaws.com controlplane.payment-cryptography.us-east-1.api.aws	HTTPS HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	controlplane.payment-cryptography.us-west-2.amazonaws.com controlplane.payment-cryptography.us-west-2.api.aws	HTTPS HTTPS
África (Ciudad del Cabo)	af-south-1	controlplane.payment-cryptography.af-south-1.amazonaws.com controlplane.payment-cryptography.af-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	controlplane.payment-cryptography.ap-south-2.amazonaws.com controlplane.payment-cryptography.ap-south-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	controlplane.payment-cryptography.ap-south-1.amazonaws.com controlplane.payment-cryptography.ap-south-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo	
Asia-Pacífico (Osaka)	ap-northeast-3	controlplane.payment-cryptography.ap-northeast-3.amazonaws.com controlplane.payment-cryptography.ap-northeast-3.api.aws	HTTPS HTTPS	
Asia-Pacífico (Singapur)	ap-southeast-1	controlplane.payment-cryptography.ap-southeast-1.amazonaws.com controlplane.payment-cryptography.ap-southeast-1.api.aws	HTTPS HTTPS	
Asia-Pacífico (Sídney)	ap-southeast-2	controlplane.payment-cryptography.ap-southeast-2.amazonaws.com controlplane.payment-cryptography.ap-southeast-2.api.aws	HTTPS HTTPS	
Asia-Pacífico (Tokio)	ap-northeast-1	controlplane.payment-cryptography.ap-northeast-1.amazonaws.com controlplane.payment-cryptography.ap-northeast-1.api.aws	HTTPS HTTPS	
Canadá (centro)	ca-central-1	controlplane.payment-cryptography.ca-central-1.amazonaws.com controlplane.payment-cryptography.ca-central-1.api.aws	HTTPS HTTPS	
Europa (Fráncfort)	eu-central-1	controlplane.payment-cryptography.eu-central-1.amazonaws.com controlplane.payment-cryptography.eu-central-1.api.aws	HTTPS HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Irlanda)	eu-west-1	controlplane.payment-cryptography.eu-west-1.amazonaws.com controlplane.payment-cryptography.eu-west-1.api.aws	HTTPS HTTPS
Europa (Londres)	eu-west-2	controlplane.payment-cryptography.eu-west-2.amazonaws.com controlplane.payment-cryptography.eu-west-2.api.aws	HTTPS HTTPS
Europa (París)	eu-west-3	controlplane.payment-cryptography.eu-west-3.amazonaws.com controlplane.payment-cryptography.eu-west-3.api.aws	HTTPS HTTPS
América del Sur (São Paulo)	sa-east-1	controlplane.payment-cryptography.sa-east-1.amazonaws.com controlplane.payment-cryptography.sa-east-1.api.aws	HTTPS HTTPS

Puntos de conexión del plano de datos

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	dataplane.payment-cryptography.us-east-2.amazonaws.com	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
		dataplane.payment-cryptography.us-east-2.api.aws	
Este de EE. UU. (Norte de Virginia)	us-east-1	dataplane.payment-cryptography.us-east-1.amazonaws.com dataplane.payment-cryptography.us-east-1.api.aws	HTTPS HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	dataplane.payment-cryptography.us-west-2.amazonaws.com dataplane.payment-cryptography.us-west-2.api.aws	HTTPS HTTPS
África (Ciudad del Cabo)	af-south-1	dataplane.payment-cryptography.af-south-1.amazonaws.com dataplane.payment-cryptography.af-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	dataplane.payment-cryptography.ap-south-2.amazonaws.com dataplane.payment-cryptography.ap-south-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Mumbai)	ap-south-1	dataplane.payment-cryptography.ap-south-1.amazonaws.com dataplane.payment-cryptography.ap-south-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Osaka)	ap-northeast-3	dataplane.payment-cryptography.ap-northeast-3.amazonaws.com dataplane.payment-cryptography.ap-northeast-3.api.aws	HTTPS HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	dataplane.payment-cryptography.ap-southeast-1.amazonaws.com dataplane.payment-cryptography.ap-southeast-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	dataplane.payment-cryptography.ap-southeast-2.amazonaws.com dataplane.payment-cryptography.ap-southeast-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	dataplane.payment-cryptography.ap-northeast-1.amazonaws.com dataplane.payment-cryptography.ap-northeast-1.api.aws	HTTPS HTTPS
Canadá (centro)	ca-central-1	dataplane.payment-cryptography.ca-central-1.amazonaws.com dataplane.payment-cryptography.ca-central-1.api.aws	HTTPS HTTPS
Europa (Fráncfort)	eu-central-1	dataplane.payment-cryptography.eu-central-1.amazonaws.com dataplane.payment-cryptography.eu-central-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Irlanda)	eu-west-1	dataplane.payment-cryptography.eu-west-1.amazonaws.com dataplane.payment-cryptography.eu-west-1.api.aws	HTTPS HTTPS
Europa (Londres)	eu-west-2	dataplane.payment-cryptography.eu-west-2.amazonaws.com dataplane.payment-cryptography.eu-west-2.api.aws	HTTPS HTTPS
Europa (París)	eu-west-3	dataplane.payment-cryptography.eu-west-3.amazonaws.com dataplane.payment-cryptography.eu-west-3.api.aws	HTTPS HTTPS
América del Sur (São Paulo)	sa-east-1	dataplane.payment-cryptography.sa-east-1.amazonaws.com dataplane.payment-cryptography.sa-east-1.api.aws	HTTPS HTTPS

Cómo empezar con la criptografía AWS de pagos

Para empezar con la criptografía de AWS pagos, primero querrá crear claves y, después, utilizarlas en diversas operaciones criptográficas. El siguiente tutorial proporciona un caso de uso sencillo para generar una clave que se utilizará para generating/verifying CVV2 los valores. Para probar otros ejemplos y explorar los patrones de implementación en AWS, visite el siguiente taller de criptografía de AWS pagos o explore nuestro proyecto de muestra disponible en GitHub

En este tutorial, se explica cómo crear una clave única y cómo realizar operaciones criptográficas con ella. Después, borra la clave si ya no la desea, completando el ciclo de vida de la clave.

> **Warning**
>
> Los ejemplos de esta guía del usuario pueden utilizar valores de muestra. Recomendamos encarecidamente no utilizar valores de muestra en un entorno de producción, como los números de serie clave.

Temas

- Requisitos previos
- Paso 1: crear una clave
- Paso 2: Genere un valor con la clave CVV2
- Paso 3: verificar el valor generado en el paso 2
- Paso 4: realizar una prueba negativa
- Paso 5: eliminación (opcional)

Requisitos previos

Antes de comenzar, asegúrese de que:

- Tiene permiso para acceder al servicio. Para obtener más información, consulte Políticas de IAM.
- Ha instalado AWS CLI. También puede utilizar AWS SDKso acceder AWS APIsa la criptografía de AWS pagos, pero en las instrucciones de este tutorial se utiliza la AWS CLI.

Paso 1: crear una clave

El primer paso es crear una clave. Para este tutorial, debe crear una clave CVK 3DES de doble longitud (2KEY TDES) para generar y verificar los valores CVV/. CVV2

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
        "KeyAttributes": {
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyAlgorithm": "TDES_2KEY",
            "KeyModesOfUse": {
                "Encrypt": false,
                "Decrypt": false,
                "Wrap": false,
                "Unwrap": false,
                "Generate": true,
                "Sign": false,
                "Verify": true,
                "DeriveKey": false,
                "NoRestrictions": false
            }
        },
        "KeyCheckValue": "CADDA1",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "Enabled": true,
        "Exportable": true,
        "KeyState": "CREATE_COMPLETE",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
        "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
    }
}
```

Tome nota de `KeyArn` que representa la clave, por ejemplo, arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi. Lo necesitará en el siguiente paso.

Paso 2: Genere un valor con la clave CVV2

En este paso, generas una CVV2 para una fecha de caducidad determinada PAN utilizando la clave del paso 1.

```
$  aws payment-cryptography-data generate-card-validation-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
    --primary-account-number=171234567890123 \
    --generation-attributes CardVerificationValue2={CardExpiryDate=0123}
```

```
{
    "CardDataGenerationKeyCheckValue": "CADDA1",
    "CardDataGenerationKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/tqv5yij6wtxx64pi",
    "CardDataType": "CARD_VERIFICATION_VALUE_2",
    "CardDataValue": "144"
}
```

Tome nota de `cardDataValue`, en este caso el número de tres dígitos 144. Lo necesitará en el siguiente paso.

Paso 3: verificar el valor generado en el paso 2

En este ejemplo, validas el dato CVV2 del paso 2 con la clave que creaste en el paso 1.

Ejecute el siguiente comando para validar el CVV2.

```
$  aws payment-cryptography-data  verify-card-validation-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
    --primary-account-number=171234567890123 \
    --verification-attributes CardVerificationValue2={CardExpiryDate=0123} \
    --validation-data 144
```

```
{
```

```
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "CADDA1"
}
```

El servicio devuelve una respuesta HTTP de 200 para indicar que ha validado la CVV2.

Paso 4: realizar una prueba negativa

En este paso, se crea una prueba negativa en la que no CVV2 es correcta ni se valida. Intenta validar un error CVV2 con la clave que creaste en el paso 1. Se trata de una operación esperada, por ejemplo, si el titular de la tarjeta ha introducido un error CVV2 al finalizar la compra.

```
$  aws payment-cryptography-data  verify-card-validation-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
    --primary-account-number=171234567890123 \
    --verification-attributes CardVerificationValue2={CardExpiryDate=0123} \
    --validation-data 999
```

```
Card validation data verification failed.
```

El servicio devuelve una respuesta HTTP de 400 con el mensaje “Fallo en la verificación de los datos de validación de la tarjeta” y el motivo INVALID_VALIDATION_DATA.

Paso 5: eliminación (opcional)

Ahora puede eliminar la clave que creó en el paso 1. Para minimizar los cambios irrecuperables, el periodo de eliminación de claves predeterminado es de siete de días.

```
$ aws payment-cryptography delete-key \
    --key-identifier=arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi
```

```
{
    "Key": {
        "CreateTimestamp": "2022-10-27T08:27:51.795000-07:00",
        "DeletePendingTimestamp": "2022-11-03T13:37:12.114000-07:00",
```

```
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
                "Wrap": true
            },
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
        },
        "KeyCheckValue": "CADDA1",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "DELETE_PENDING",
        "UsageStartTimestamp": "2022-10-27T08:27:51.753000-07:00"
    }
}
```


Tome nota de dos campos en la salida. El `deletePendingTimestamp` se fija por defecto para los siete días posteriores. El KeyState está establecido en `DELETE_PENDING`. Puede cancelar esta eliminación en cualquier momento antes de la hora de eliminación programada llamando al `restore-key`.

Administración de claves

Para empezar a utilizar la criptografía AWS de pagos, cree una clave de criptografía AWS de pagos.

En esta sección se explica cómo crear y administrar varios tipos de claves de criptografía de AWS pagos a lo largo de su ciclo de vida. Aprenderás a crear, ver y editar claves, así como a etiquetarlas, crear alias de claves y activar o desactivar claves.

Una clave AWS de criptografía de pagos es un recurso regional. Si tiene intención de utilizar una clave determinada de forma múltiple Regiones de AWS, puede habilitar la replicación de Multi-Region claves, que copia de forma segura el material clave y los metadatos Regiones de AWS que especifique dentro de la misma AWS partición y cuenta. La clave de origen en la replicación de Multi-Region claves se conoce como clave de región principal (PRK) y sigue siendo la fuente autorizada para todas las actividades de administración de claves. La clave replicada se conoce como clave de región de réplica (RRK) y es una réplica de solo lectura de la PRK. Deberías considerar la posibilidad de usar Multi-Region claves con tus claves para cumplir con los objetivos de diseño relacionados con la disponibilidad, la recuperación ante desastres y la baja latencia.

Temas

- Crear claves
- Enumerar las claves
- Habilitación y desactivación de claves de
- Replicación de claves de criptografía AWS de pago
- Eliminación de claves de
- Importación y exportación de claves
- Uso de alias
- Obtener claves
- Etiquetado de claves
- Comprender los atributos clave de la clave AWS de criptografía de pagos

Crear claves

Puede crear claves de criptografía de AWS pagos mediante la operación de la CreateKey API. Al crear una clave, se especifican atributos como el algoritmo de la clave, el uso de la clave, las

operaciones permitidas y si es exportable. No puedes cambiar estas propiedades después de crear la clave de criptografía AWS de pagos.

> **Note**
>
> Si habilita la replicación de Multi-Region claves Cuenta de AWS y crea una clave de criptografía de pagos, esta clave se convertirá automáticamente en una clave de región principal (PRK). La PRK se replica incluso si no se especifica el `--replication-regions` parámetro en el comando. CreateKey Para obtener más información, consulte Cómo funciona la replicación de Multi-Region claves.

Ejemplos

- Creación de una clave de derivación base TDES de 3 teclas
- Crear una clave TDES de 2 teclas para CVV/CVV2
- Crear una clave HMAC
- Crear una clave AES-256
- Creación de una clave de cifrado PIN (PEK)
- Crear una clave asimétrica (RSA)
- Creación de una clave de valor de verificación de PIN (PVV)
- Crear una clave ECC asimétrica

Creación de una clave de derivación base TDES de 3 teclas

Example

Este comando crea una clave de derivación TDES de 3 teclas que se replicará en las regiones EE.UU. Este (Ohio) y EE.UU. Oeste (Oregón). La respuesta incluye los parámetros de la solicitud, un nombre de recurso de Amazon (ARN) para las llamadas posteriores y un valor de comprobación clave (KCV).

```
$ aws payment-cryptography create-key --exportable --key-attributes \
     "KeyUsage=TR31_B0_BASE_DERIVATION_KEY, \
     KeyClass=SYMMETRIC_KEY,KeyAlgorithm=TDES_3KEY, \
     KeyModesOfUse={NoRestrictions=true}" \
     --replication-regions us-east-2 --region us-west-2
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2022-10-26T16:04:11.642000-07:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "FE23D3",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": true,
                "Encrypt": false,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_B0_BASE_DERIVATION_KEY"
        },
        "KeyCheckValue": "FE23D3",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2022-10-26T16:04:11.559000-07:00"
}
```

Crear una clave TDES de 2 teclas para CVV/CVV2

Example

Este comando crea una clave TDES de 2 teclas para generar y verificar valores. CVV/CVV2 La respuesta incluye los parámetros de la solicitud, un nombre de recurso de Amazon (ARN) para las llamadas posteriores y un valor de comprobación clave (KCV).

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY, \
    KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY, \
    KeyModesOfUse='{Generate=true,Verify=true}'
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2022-10-26T16:04:11.642000-07:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/7f7g4spf3xcklhzu",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
        },
        "KeyCheckValue": "AEA5CD",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2022-10-26T16:04:11.559000-07:00"
    }
}
```

Crear una clave HMAC

Example

Las claves HMAC se utilizan para generar o verificar los códigos de autenticación de mensajes hash (HMAC). En el caso de las claves HMAC, el tipo de hash se asigna en el momento de la creación de la clave (por ejemplo, HMAC_SHA224 y HMAC_SHA512) y no se puede modificar.

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=HMAC_SHA512,KeyUsage=TR31_M7_HMAC_KEY,KeyClass=SYMMETRIC_KEY,KeyModesOfUse='{Gene
 = true,Verify = true}'
```

Ejemplo de código de salida:

```
{
 "Key": {
 "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/qnobl5lghrzunce6",
 "KeyAttributes": {
 "KeyUsage": "TR31_M7_HMAC_KEY",
 "KeyClass": "SYMMETRIC_KEY",
 "KeyAlgorithm": "HMAC_SHA512",
 "KeyModesOfUse": {
 "Encrypt": false,
 "Decrypt": false,
 "Wrap": false,
 "Unwrap": false,
 "Generate": true,
 "Sign": false,
 "Verify": true,
 "DeriveKey": false,
 "NoRestrictions": false
 }
 },
 "KeyCheckValue": "2976E7",
 "KeyCheckValueAlgorithm": "HMAC",
 "Enabled": true,
 "Exportable": true,
 "KeyState": "CREATE_COMPLETE",
 "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
 "CreateTimestamp": "2025-07-30T10:06:12.142000-07:00",
 "UsageStartTimestamp": "2025-07-30T10:06:12.128000-07:00"
 }
}
```

Crear una clave AES-256

Example

Este comando crea una clave AES-256 simétrica para el cifrado y descifrado de datos. Las claves AES proporcionan un cifrado seguro para los datos confidenciales y, por lo general, se utilizan en el procesamiento de pagos para cifrar los datos de los titulares de las tarjetas y otra información confidencial; sin embargo, el TDES se usa más comúnmente para casos de uso de emisores como el EMV.

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=AES_256,KeyUsage=TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY,KeyClass=SYMMETRIC_KEY,Key
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2025-02-02T10:15:30.142000-08:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-1:111122223333:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyAlgorithm": "AES_256",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
                "Wrap": true
            },
            "KeyUsage": "TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY"
        },
        "KeyCheckValue": "2976F5",
        "KeyCheckValueAlgorithm": "CMAC",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2025-02-02T10:15:30.128000-08:00"
    }
}
```

Creación de una clave de cifrado PIN (PEK)

Example

Este comando crea una clave TDES de 3 teclas para cifrar los valores del PIN, aunque las claves PIN también pueden ser AES, según la necesidad de interoperabilidad. Puede usar esta clave para almacenar los PIN de forma segura o para descifrar los PIN durante la verificación, por ejemplo, en una transacción. La respuesta incluye los parámetros de la solicitud, un ARN para las llamadas posteriores y un KCV.

```
$ aws payment-cryptography create-key --exportable --key-attributes \
    KeyAlgorithm=TDES_3KEY,KeyUsage=TR31_P0_PIN_ENCRYPTION_KEY, \

 KeyClass=SYMMETRIC_KEY,KeyModesOfUse='{Encrypt=true,Decrypt=true,Wrap=true,Unwrap=true}'
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2022-10-27T08:27:51.795000-07:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
                "Wrap": true
            },
            "KeyUsage": "TR31_P0_PIN_ENCRYPTION_KEY"
        },
        "KeyCheckValue": "7CC9E2",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2022-10-27T08:27:51.753000-07:00"
    }
}
```

Crear una clave asimétrica (RSA)

Example

Este comando genera un nuevo key pair asimétrico RSA de 2048 bits. Crea una nueva clave privada y su clave pública correspondiente. Puede recuperar la clave pública mediante la PublicCertificate API get.

```
$ aws payment-cryptography create-key --exportable \
    --key-attributes
 KeyAlgorithm=RSA_2048,KeyUsage=TR31_D1_ASYMMETRIC_KEY_FOR_DATA_ENCRYPTION, \
    KeyClass=ASYMMETRIC_KEY_PAIR,KeyModesOfUse='{Encrypt=true,
 Decrypt=True,Wrap=True,Unwrap=True}'
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2022-11-15T11:15:42.358000-08:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
nsq2i3mbg6sn775f",
        "KeyAttributes": {
            "KeyAlgorithm": "RSA_2048",
            "KeyClass": "ASYMMETRIC_KEY_PAIR",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
                "Wrap": true
            },
            "KeyUsage": "TR31_D1_ASYMMETRIC_KEY_FOR_DATA_ENCRYPTION"
        },
        "KeyCheckValue": "40AD487F",
        "KeyCheckValueAlgorithm": "SHA-1",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2022-11-15T11:15:42.182000-08:00"
    }
}
```

Creación de una clave de valor de verificación de PIN (PVV)

Example

Este comando crea una clave TDES de 3 teclas para generar valores de PVV. Puede utilizar esta clave para generar un PVV que se pueda comparar con un PVV calculado posteriormente. La respuesta incluye los parámetros de la solicitud, un ARN para las llamadas posteriores y un KCV.

```
$ aws payment-cryptography create-key --exportable \
    --key-attributes KeyAlgorithm=TDES_3KEY,KeyUsage=TR31_V2_VISA_PIN_VERIFICATION_KEY,
 \
    KeyClass=SYMMETRIC_KEY,KeyModesOfUse='{Generate=true,Verify=true}'
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2022-10-27T10:22:59.668000-07:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_V2_VISA_PIN_VERIFICATION_KEY"
        },
        "KeyCheckValue": "7F2363",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2022-10-27T10:22:59.614000-07:00"
    }
}
```

Crear una clave ECC asimétrica

Example

Este comando genera un par de claves ECC para establecer un acuerdo de claves ECDH (curva elíptica Diffie-Hellman) entre dos partes. Con el ECDH, cada parte genera su propio par de claves ECC con el propósito clave K3 y el modo de uso X, e intercambian claves públicas. A continuación, ambas partes utilizan su clave privada y la clave pública recibida para establecer una clave derivada compartida.

Para mantener el principio de un solo uso de las claves criptográficas en los pagos, recomendamos no reutilizar los pares de claves ECC para varios fines, como la obtención y firma de claves ECDH.

```
$ aws payment-cryptography create-key --exportable \
    --key-attributes
 KeyAlgorithm=ECC_NIST_P256,KeyUsage=TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT, \
    KeyClass=ASYMMETRIC_KEY_PAIR,KeyModesOfUse='{DeriveKey=true}'
```

Ejemplo de código de salida:

```
{
    "Key": {
        "CreateTimestamp": "2024-10-17T01:31:55.908000+00:00",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
wc3rjsssguhxtilv",
        "KeyAttributes": {
            "KeyAlgorithm": "ECC_NIST_P256",
            "KeyClass": "ASYMMETRIC_KEY_PAIR",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": true,
                "Encrypt": false,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": false,
                "Wrap": false
            },
            "KeyUsage": "TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT"
        },
        "KeyCheckValue": "7E34F19F",
        "KeyCheckValueAlgorithm": "SHA-1",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2024-10-17T01:31:55.866000+00:00"
    }
}
```

Enumerar las claves

Utilice esta ListKeys operación para obtener una lista de claves a las que pueda acceder en su cuenta y región.

Example

```
$ aws payment-cryptography list-keys
```

Ejemplo de código de salida:

```
{
    "Keys": [
        {
            "CreateTimestamp": "2022-10-12T10:58:28.920000-07:00",
            "Enabled": false,
            "Exportable": true,
            "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
            "KeyAttributes": {
                "KeyAlgorithm": "TDES_3KEY",
                "KeyClass": "SYMMETRIC_KEY",
                "KeyModesOfUse": {
                    "Decrypt": true,
                    "DeriveKey": false,
                    "Encrypt": true,
                    "Generate": false,
                    "NoRestrictions": false,
                    "Sign": false,
                    "Unwrap": true,
                    "Verify": false,
                    "Wrap": true
                },
                "KeyUsage": "TR31_P1_PIN_GENERATION_KEY"
            },
            "KeyCheckValue": "7F2363",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "KeyState": "CREATE_COMPLETE",
            "UsageStopTimestamp": "2022-10-27T14:19:42.488000-07:00"
        }
    ]
}
```

Habilitación y desactivación de claves de

Puede deshabilitar y volver a activar las claves de criptografía AWS de pagos. Al crear una clave, se habilita de forma predeterminada. Si deshabilita una clave, no podrá utilizarla en ninguna operación criptográfica hasta que la vuelva a activar. Start/stop Los comandos de uso tienen efecto inmediato, por lo que se recomienda revisar el uso antes de realizar dichos cambios. También puede establecer un cambio (iniciar o detener el uso) para que surta efecto en el futuro utilizando el parámetro `timestamp` opcional.

Como es temporal y se deshace fácilmente, deshabilitar una clave de criptografía de AWS pago es una alternativa más segura que eliminarla, una acción destructiva e irreversible. AWS Si está pensando en eliminar una clave de criptografía de AWS pagos, desactívela primero y asegúrese de que no necesitará utilizarla para cifrar o descifrar datos en el futuro.

Temas

- Iniciar el uso de claves
- Detener el uso de claves

Iniciar el uso de claves

El uso de claves debe estar habilitado para poder utilizar una clave para operaciones criptográficas. Si una clave no está habilitada, puede utilizar esta operación para hacerla utilizable. El campo `UsageStartTimestamp` representará cuándo se activará la clave became/will . Esto será en el pasado para un token habilitado, y en el futuro si está pendiente de activación.

Example

En este ejemplo, se solicita la habilitación de una llave para su uso. La respuesta incluye la información de la llave y el indicador de habilitación ha pasado a verdadero. Esto también se reflejará en el objeto de respuesta lista-claves.

```
$ aws payment-cryptography start-key-usage --key-identifier "arn:aws:payment-
cryptography:us-east-2:111122223333:key/alsuwfxug3pgy6xh"
```

```
{
      "Key": {
      "CreateTimestamp": "2022-10-12T10:58:28.920000-07:00",
      "Enabled": true,
      "Exportable": true,
      "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh",
      "KeyAttributes": {
          "KeyAlgorithm": "TDES_3KEY",
          "KeyClass": "SYMMETRIC_KEY",
          "KeyModesOfUse": {
              "Decrypt": true,
              "DeriveKey": false,
              "Encrypt": true,
              "Generate": false,
              "NoRestrictions": false,
              "Sign": false,
              "Unwrap": true,
              "Verify": false,
              "Wrap": true
          },
          "KeyUsage": "TR31_P1_PIN_GENERATION_KEY"
      },
      "KeyCheckValue": "369D",
      "KeyCheckValueAlgorithm": "ANSI_X9_24",
      "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
      "KeyState": "CREATE_COMPLETE",
      "UsageStartTimestamp": "2022-10-27T14:09:59.468000-07:00"
  }
}
```

Detener el uso de claves

Si ya no tiene previsto utilizar una clave, puede detener el uso de la clave para evitar que se realicen más operaciones criptográficas. Esta operación no es permanente, por lo que puede revertirla utilizando iniciar uso de clave. También puede configurar una clave para que se desactive en el futuro. El campo `UsageStopTimestamp` representará el momento en que la clave became/will se desactive.

Example

En este ejemplo, se solicita detener el uso de la llave en el futuro. Tras la ejecución, esta clave no podrá utilizarse para operaciones criptográficas a menos que se vuelva a habilitar mediante iniciar uso de clave. La respuesta incluye la información de la clave y que el indicador de habilitación haya pasado a falso. Esto también se reflejará en el objeto de respuesta lista-claves.

```
$ aws payment-cryptography stop-key-usage --key-identifier "arn:aws:payment-
cryptography:us-east-2:111122223333:key/alsuwfxug3pgy6xh"
```


```
{
  "Key": {
      "CreateTimestamp": "2022-10-12T10:58:28.920000-07:00",
      "Enabled": false,
      "Exportable": true,
      "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh",
      "KeyAttributes": {
          "KeyAlgorithm": "TDES_3KEY",
          "KeyClass": "SYMMETRIC_KEY",
          "KeyModesOfUse": {
              "Decrypt": true,
              "DeriveKey": false,
              "Encrypt": true,
              "Generate": false,
              "NoRestrictions": false,
              "Sign": false,
              "Unwrap": true,
              "Verify": false,
              "Wrap": true
          },
          "KeyUsage": "TR31_P1_PIN_GENERATION_KEY"
      },
      "KeyCheckValue": "369D",
      "KeyCheckValueAlgorithm": "ANSI_X9_24",
      "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
      "KeyState": "CREATE_COMPLETE",
      "UsageStopTimestamp": "2022-10-27T14:09:59.468000-07:00"
  }
}
```

Replicación de claves de criptografía AWS de pago

AWS La criptografía de pago admite la replicación de Multi-Region claves, lo que le permite distribuir de forma segura el material clave y los metadatos de cualquier clave de criptografía de AWS pago determinada a una o más de las Regiones de AWS mismas AWS particiones y cuentas.

La clave de origen se conoce como clave de región principal (PRK) y sigue siendo la fuente autorizada para todas las actividades de administración de claves, mientras que tanto la clave PRK como la clave de región de réplica (RRK) se pueden utilizar para las operaciones criptográficas respectivas. Regiones de AWS

Ventajas de la replicación de claves Multi-Region

A continuación, se describen algunos de los beneficios de la replicación de Multi-Region claves.

- Configuración más sencilla para aplicaciones de alta disponibilidad: la criptografía de AWS pagos se encarga de la distribución de claves para que pueda utilizar una clave en varias unidades Regiones de AWS sin necesidad de crear copias disociadas de una clave determinada.
- Claves de alta disponibilidad y baja latencia: con Multi-Region la replicación de claves, puede acceder a sus claves en varias, Regiones de AWS lo que hace que tengan una alta disponibilidad, lo que reduce la latencia.
- Durabilidad del material clave: las claves de región de réplica son réplicas de claves completas y se pueden utilizar independientemente de su clave de región principal en las operaciones criptográficas. Una RRK proporciona una réplica duradera en caso de una pérdida de datos catastrófica de una PRK.

Cómo funciona la replicación de Multi-Region claves

Cuando la replicación de Multi-Region claves está habilitada, el servicio de criptografía de AWS pagos utiliza mecanismos seguros de distribución de claves para copiar el material clave y los metadatos a la réplica Regiones de AWS que especifique. Los cambios en los metadatos clave de una región principal, como los atributos clave, el estado y la habilitación, se replican automáticamente en las claves de la región de la réplica.

Limitaciones y consideraciones

A continuación, se indican algunas limitaciones y Multi-Region consideraciones clave sobre la replicación.

- Debe habilitar esta función para una Región de AWS o varias claves de criptografía de pago específicas.
  - Si esta función está habilitada para una Región de AWS, todas las claves de criptografía de AWS pagos creadas después de la activación se replicarán en las especificadas. Región de AWS Las claves creadas en esta región se convertirán en claves de la región principal. Las claves existentes en esta región no se replicarán automáticamente. Puede habilitar la replicación de Multi-Region claves para las claves existentes dentro de un Región de AWS nivel de clave.
  - Cada uno Región de AWS puede tener una configuración de replicación de Multi-Region claves única.
  - La configuración de Multi-Region replicación de una clave tiene prioridad sobre la configuración de replicación de Región de AWS Multi-Region claves.
- No se puede configurar una clave de región de réplica para que se replique en otra Regiones de AWS.
- Multi-Region La replicación de claves está disponible para claves de criptografía de pagos simétricas, como el estándar de cifrado triple de datos (3DES), el estándar de cifrado avanzado (AES) y el código de autenticación de Hash-based mensajes (HMAC).
- Las claves de criptografía de pago asimétricas no admiten la replicación de claves. Multi-Region
- Las claves de región de réplica son claves de solo lectura. Todos los cambios en la clave de región principal se aplicarán a las claves de región de réplica.
- En última instancia, los cambios en la clave de región principal son coherentes con las claves de región de la réplica.
- Las claves de criptografía de pago solo se pueden replicar con la misma AWS partición y cuenta.
- Las claves de Réplica Region cuentan para el límite de criptografía Cuenta de AWS de AWS pagos de su nivel.
- La clave de región principal y la clave de región de réplica utilizan el mismo identificador de clave, lo que le permite hacer referencia a ambas claves mediante el mismo ARN en las políticas de IAM.
- Debe tener `CreateKey` permisos en la réplica Región de AWS para que la replicación se realice correctamente.

Habilitar Multi-Region la replicación de claves

Hay dos formas de habilitar la replicación de Multi-Region claves para las claves de criptografía de AWS pagos.

1. Región de AWS: Multi-Region la replicación de claves se aplica a todas las claves nuevas que se creen en ella Región de AWS cuando está habilitada. Este método proporciona una replicación uniforme para todas las claves.
2. Claves AWS de criptografía de pago específicas: puede gestionar Multi-Region la replicación de claves individuales, lo que permite un nivel de control más detallado.

Una vez habilitada la replicación de Multi-Region claves, sus claves de criptografía de pago se replicarán según Regiones de AWS lo que especifique.

> **Important**
>
> Multi-Region la replicación de claves no se puede pausar. Las claves se replican automáticamente según Regiones de AWS lo especificado una vez que se habilita la replicación. Multi-Region la replicación de claves se puede deshabilitar para una clave de criptografía específica Región de AWS o de pago. Debe eliminar la Región de AWS como región de replicación de la clave de región principal para eliminar la clave de región de réplica.
> Como alternativa, puede llamar al comando `StopKeyUsage`API o stop-key-usageCLI de su PRK para detener el uso tanto de la PRK como de todas las RRK asociadas. No podrás usar estas claves en operaciones criptográficas. El uso de un comando `StopKeyUsage` API o stop-key-usage CLI no detendrá la replicación de Multi-Region claves en curso habilitada para su PRK.

Puede comprobar la configuración de replicación de Multi-Region claves para las claves de criptografía de AWS pago en un lugar específico Región de AWS llamando al comando `GetDefaultKeyReplicationRegions` API o get-default-key-replication-regions CLI. Las claves Región de AWS donde llames a esta acción o comando de la API se convertirán en tu PRK.

Utilice los siguientes procedimientos para habilitar la replicación de Multi-Region claves.

For Región de AWS

- Utilice el siguiente comando para habilitar la replicación de Multi-Region claves para una clave Región de AWS que especifique. En este ejemplo, la replicación de Multi-Region claves está habilitada en EE. UU. Este (Ohio) y EE. UU. Oeste (Oregón). Para usar este comando, sustituya *`italicized placeholder text`* el comando del ejemplo por su propia información.

```
aws payment-cryptography enable-default-key-replication-regions \
    --replication-regions us-east-2 us-west-2
```

> **Note**
>
> Si se habilita la replicación de Multi-Region claves para un, no Región de AWS se cambiará la configuración de replicación de ninguna de las claves de criptografía de AWS pagos existentes. Puede activar esta función para las claves existentes a nivel de clave. Solo las claves creadas después Multi-Region de activar la replicación de claves Región de AWS utilizarán la configuración de replicación regional.

For specific AWS Payment Cryptography keys

- Utilice el siguiente comando para habilitar la replicación de Multi-Region claves de criptografía de pago específicas. En este ejemplo, la replicación de Multi-Region claves está habilitada en el este de EE. UU. (Ohio). Para usar este comando, sustituya *italicized placeholder text* el comando del ejemplo por su propia información.

  ```
  aws payment-cryptography add-key-replication-regions \
      --key-identifier arn:aws:payment-cryptography:us-
  east-2:111122223333:key/kwapwa6qaifllw2h \
      --replication-regions us-east-2
  ```

Como alternativa, puede crear una nueva clave de criptografía de pagos con esta función habilitada e incluir la replicación Regiones de AWS en su solicitud de creación de clave.

> **Note**
>
> La configuración de replicación de claves tiene prioridad sobre la configuración de Región de AWS replicación.

Deshabilitar Multi-Region la replicación de claves

Si desea deshabilitar la replicación de Multi-Region claves, puede llamar a los comandos disable-default-key-replication o a los comandos remove-key-replication-regions CLI, según cómo esté habilitada la replicación de Multi-Region claves. Deberá especificar el ARN de la clave y deshabilitar la replicación Región de AWS de Multi-Region claves.

Consideraciones

En última instancia, las eliminaciones de claves de la región de replicación son consistentes.

Puede comprobar la configuración de replicación de Multi-Region claves para las claves de criptografía de AWS pago en un lugar específico Región de AWS llamando al comando `GetDefaultKeyReplicationRegions` API o get-default-key-replication-regions CLI.

Utilice los siguientes procedimientos para deshabilitar la replicación de Multi-Region claves.

For Región de AWS

- Utilice el siguiente comando para deshabilitar la replicación de Multi-Region claves de una clave Región de AWS que especifique. En este ejemplo, la replicación de Multi-Region claves está deshabilitada en el este de EE. UU. (Ohio). Para usar este comando, sustituya *italicized placeholder text* el comando del ejemplo por su propia información.

```
aws payment-cryptography disable-default-key-replication-regions \
    --replication-regions us-east-2
```

For specific AWS Payment Cryptography keys

- Use el siguiente comando para deshabilitar la replicación de Multi-Region claves para una clave de criptografía de pagos específica. En este ejemplo, la replicación de Multi-Region claves está deshabilitada en el este de EE. UU. (Ohio). Para usar este comando, sustituya *italicized placeholder text* el comando del ejemplo por su propia información.

```
aws payment-cryptography remove-key-replication-regions \
    --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h \
    --replication-regions us-east-2
```

Consideraciones de seguridad

Las siguientes son consideraciones de seguridad a la hora de utilizar la replicación de Multi-Region claves para las claves de criptografía de pagos. Para obtener más información, consulte Prácticas recomendadas de seguridad para la criptografía AWS de pagos.

- Limite el intercambio de materiales clave.
- Siga el principio de permisos con privilegios mínimos al crear políticas de IAM.
- No puede realizar cambios en la clave de región de réplica, ya que es una clave de solo lectura.

Prácticas recomendadas

Las siguientes son algunas de las mejores prácticas a la hora de utilizar la replicación de Multi-Region claves con claves de criptografía AWS de pagos.

- Asegúrese de que su aplicación siga funcionando incluso si la replicación de la Multi-Region clave especificada no Región de AWS es inmediata. Si necesita saber cuándo se ha completado la replicación de Multi-Region claves, puede monitorizarla con la acción de la GetKeyAPI. Puede supervisar los eventos de replicación de claves con AWS CloudTrail.
- Pruebe e implemente procesos de implementación automatizados en caso de conmutación por error de una región Región de AWS a otra.

Precios

Se le cobrará por las réplicas de claves de región que cree con AWS Payment Cryptography. Estas claves se cobran por. Región de AWS Para obtener la información más reciente sobre los precios de la criptografía de pagos, consulta la página de precios AWS de la criptografía de pagos.

Eliminación de claves de

Al eliminar una clave de criptografía de AWS pago, se eliminan el material de la clave y todos los metadatos asociados a la clave y es irreversible, a menos que haya una copia de la clave disponible fuera de la criptografía de AWS pago. Una vez que se elimina una clave, ya no pueden descifrar los datos que se habían cifrado con ella, lo que significa que los datos pueden volverse irrecuperables. Sólo debe eliminar una clave cuando esté seguro de que ya no necesita utilizarla y de que no hay terceros que la estén utilizando. Si no está seguro, considere la posibilidad de interrumpir el uso de

la clave en lugar de eliminarla. Puedes volver a activar una clave desactivada si necesitas volver a utilizarla más adelante, pero no podrás recuperar una clave de criptografía de AWS pagos eliminada a menos que puedas volver a importarla desde otra fuente.

Antes de eliminar una clave, asegúrate de que ya no la necesitas. AWS La criptografía de pagos no almacena los resultados de las operaciones criptográficas, como ocurre con el CVV2, y no puede determinar si se necesita una clave para cualquier material criptográfico persistente.

AWS La criptografía de pagos nunca elimina las claves que pertenecen a las AWS cuentas activas, a menos que se programe explícitamente su eliminación y caduque el período de espera obligatorio.

Sin embargo, puede optar por eliminar una clave de criptografía de AWS pago por uno o varios de los siguientes motivos:

- Para completar el ciclo de vida de una clave que ya no necesita
- Para evitar los gastos de administración asociados con el mantenimiento de las claves de criptografía AWS de pago no utilizadas

> **Note**
>
> Si cierras o eliminas la tuya Cuenta de AWS, tu clave de criptografía de AWS pago quedará inaccesible. No necesita programar la eliminación de su clave de criptografía de AWS pago aparte del cierre de la cuenta.

AWS La criptografía de pagos registra una entrada en su AWS CloudTrailregistro cuando programa la eliminación de la clave de criptografía de AWS pagos y cuando se elimina realmente la clave de criptografía de AWS pagos.

Cuando se utiliza la replicación de Multi-Region claves y se elimina una clave de criptografía de pago que sea una clave de región principal (PRK), las claves de región de réplica (RRK) también se eliminarán automáticamente. Una RRK no se puede eliminar como una PRK. Si desea eliminar una RRK, tendrá que modificar las regiones de replicación de su PRK.

Acerca del período de espera

Como eliminar una clave es irreversible, la criptografía de AWS pagos requiere que establezcas un período de espera de entre 3 y 180 días. El periodo de espera predeterminado es de siete días.

Sin embargo, el período de espera real puede ser hasta 24 horas más largo que el programado. Para obtener la fecha y la hora reales en las que se eliminará la clave de criptografía de AWS pago, utilice las siguientes operaciones. GetKey Asegúrese de anotar la zona horaria.

Durante el período de espera, el estado de la clave AWS de criptografía de pago y el estado de la clave es Pendiente de eliminación.

> **Note**
>
> Una clave AWS de criptografía de pago pendiente de eliminación no se puede utilizar en ninguna operación criptográfica.

Una vez finalizado el período de espera, la criptografía de AWS pago elimina la clave de criptografía de AWS pago, sus alias y todos los metadatos de criptografía de pago relacionados. AWS

Utilice el período de espera para asegurarse de que no necesitará la clave de criptografía de AWS pago ahora o en el futuro. Si se da cuenta de que necesita la clave durante el periodo de espera, puede cancelar la eliminación de la clave antes de que finalice el periodo de espera. Una vez que finaliza el periodo de espera, no puede cancelar la eliminación de claves y el servicio elimina la clave.

Example

En este ejemplo, se solicita la eliminación de una clave. Además de la información clave básica, hay dos campos importantes: que el estado de la clave se ha cambiado a DELETE_PENDING y eliminar PendingTimestamp representa el momento en el que está programada la eliminación de la clave en ese momento.

```
$ aws payment-cryptography delete-key \
                    --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h
```

```
  {
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_V2_VISA_PIN_VERIFICATION_KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyAlgorithm": "TDES_3KEY",
            "KeyModesOfUse": {
                "Encrypt": false,
                "Decrypt": false,
                "Wrap": false,
                "Unwrap": false,
                "Generate": true,
                "Sign": false,
                "Verify": true,
                "DeriveKey": false,
                "NoRestrictions": false
            }
        },
        "KeyCheckValue": "0A3674",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "Enabled": false,
        "Exportable": true,
        "KeyState": "DELETE_PENDING",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "CreateTimestamp": "2023-06-05T12:01:29.969000-07:00",
        "UsageStopTimestamp": "2023-06-05T14:31:13.399000-07:00",
        "DeletePendingTimestamp": "2023-06-12T14:58:32.865000-07:00"
    }
}
```

Example

En este ejemplo, se cancela un borrado pendiente. Una vez completada con éxito, la clave ya no se borrará según la programación anterior. La respuesta contiene la información básica de la clave; además, han cambiado dos campos relevantes: `KeyState` y `deletePendingTimestamp`. `KeyState` se devuelve a un valor de CREATE_COMPLETE, mientras que `DeletePendingTimestamp` se elimina.

```
$ aws payment-cryptography restore-key --key-identifier arn:aws:payment-
cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h
```

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_V2_VISA_PIN_VERIFICATION_KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyAlgorithm": "TDES_3KEY",
            "KeyModesOfUse": {
                "Encrypt": false,
                "Decrypt": false,
                "Wrap": false,
                "Unwrap": false,
                "Generate": true,
                "Sign": false,
                "Verify": true,
                "DeriveKey": false,
                "NoRestrictions": false
            }
        },
        "KeyCheckValue": "0A3674",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "Enabled": false,
        "Exportable": true,
        "KeyState": "CREATE_COMPLETE",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "CreateTimestamp": "2023-06-08T12:01:29.969000-07:00",
        "UsageStopTimestamp": "2023-06-08T14:31:13.399000-07:00"
    }
}
```

Importación y exportación de claves

Puede importar claves de criptografía de AWS pagos desde otras soluciones y exportarlas a otras soluciones, como los HSM. Muchos clientes intercambian claves con los proveedores de servicios mediante la funcionalidad de importación y exportación. Diseñamos la criptografía de AWS pagos para utilizar un enfoque electrónico moderno en la gestión de claves que le ayude a mantener el cumplimiento y los controles. Recomendamos utilizar el intercambio electrónico de claves basado en estándares en lugar de componentes clave en papel. Si necesita seguir procesando componentes clave en papel hasta que todos los socios admitan el intercambio electrónico de claves, puede utilizarIntercambio de claves físicas.

Puntos clave mínimos y efecto en las funciones de importación y exportación

La PCI requiere fortalezas clave mínimas específicas para las operaciones criptográficas, el almacenamiento y la transmisión de claves. Estos requisitos pueden cambiar cuando se revisan los estándares de PCI. Las normas especifican que el embalaje de las llaves utilizadas para el almacenamiento o el transporte debe ser al menos tan resistente como la clave que se está protegiendo. Aplicamos este requisito automáticamente durante la exportación y evitamos que las claves estén protegidas por claves más débiles, como se muestra en la siguiente tabla.

En la siguiente tabla se muestran las combinaciones admitidas de llaves para envolver, llaves para proteger y métodos de protección.

	Llave de embalaje											
Clave para proteger	TDES	TDES	AES_	AES_	AES_	RSA_	RSA_	RSA_	ECC_	ECC_	ECC_	Notas
TDES_2KE	TR-3	TR-3	TR-3	TR-3	TR-3	TR-3 RSA	TR-3 RSA	TR-3 RSA	ECDI	ECDI	ECDI	
CLAVE TDES_3	✗ No se admi	TR-3	TR-3	TR-3	TR-3	TR-3 RSA	TR-3 RSA	TR-3 RSA	ECDI	ECDI	ECDI	
AES_128	✗ No	✗ No	TR-3	TR-3	TR-3	✗ No	TR-3 RSA	TR-3 RSA	ECDI	ECDI	ECDI	

	Llave de embalaje											
Clave para proteger	TDES compe	TDES se admit	AES_	AES_	AES_	RSA_ se admit	RSA_	RSA_	ECC_	ECC_	ECC_	Notas
AES_192	✗ No compe	✗ No se admit	✗ No se admit	TR-3	TR-3	✗ No se admit	✗ No se admit	✗ No se admit	✗ No se admit	ECDI	ECDI	
AES_256	✗ No compe	✗ No se admit	✗ No se admit	✗ No se admit	TR-3	✗ No se admit	✗ No se admit	✗ No se admit	✗ No se admit	✗ No se admit	ECDI	

Para obtener más información, consulte el apéndice D: Tamaños y fortalezas de clave mínimos y equivalentes para los algoritmos aprobados en las normas PCI HSM.

Intercambio de claves de cifrado (KEK)

Recomendamos utilizar el estándar X9.24 TR-34ANSI. Este tipo de clave inicial puede denominarse clave de cifrado de clave (KEK), clave maestra de zona (ZMK) o clave maestra de control de zona (ZCMK). Si sus sistemas o socios TR-34 aún no son compatibles, puede usar RSA. Wrap/Unwrap Si sus necesidades incluyen el intercambio de AES-256 claves, puede utilizar el ECDH.

> **Note**
>
> Para importar sus propias claves de prueba o sincronizarlas con sus HSM existentes, consulte el código de ejemplo de criptografía de AWS pagos que aparece en. GitHub

Intercambio de claves de trabajo (WK)

Utilizamos los estándares del sector (ANSI X9.24 TR 31-2018 y X9.143) para intercambiar las claves de trabajo. Para ello, es necesario que ya haya intercambiado una KEK mediante RSA Wrap TR-34, ECDH o esquemas similares. Este enfoque cumple con el requisito del PIN PCI para vincular criptográficamente el material clave según su tipo y uso en todo momento. Las claves de trabajo incluyen las claves de trabajo del adquirente, las claves de trabajo del emisor, el BDK y el IPEK.

Temas

- Importar claves
- Exportar claves
- Temas avanzados

Importar claves

> **Important**
>
> Los ejemplos requieren la versión más reciente de la AWS CLI V2. Antes de empezar, asegúrese de haber actualizado a la versión más reciente.

Contenido

- Introducción a la importación de claves
- Importar claves simétricas
  - Importe claves mediante técnicas asimétricas () TR-34
  - Importe las claves mediante técnicas asimétricas (ECDH)
  - Importe las claves mediante técnicas asimétricas (RSA Unwrap)
  - Importe claves simétricas mediante una clave de intercambio de claves preestablecida () TR-31
- Importación de claves públicas asimétricas (RSA, ECC)
  - Importar claves públicas RSA
  - Importación de claves públicas ECC

Introducción a la importación de claves

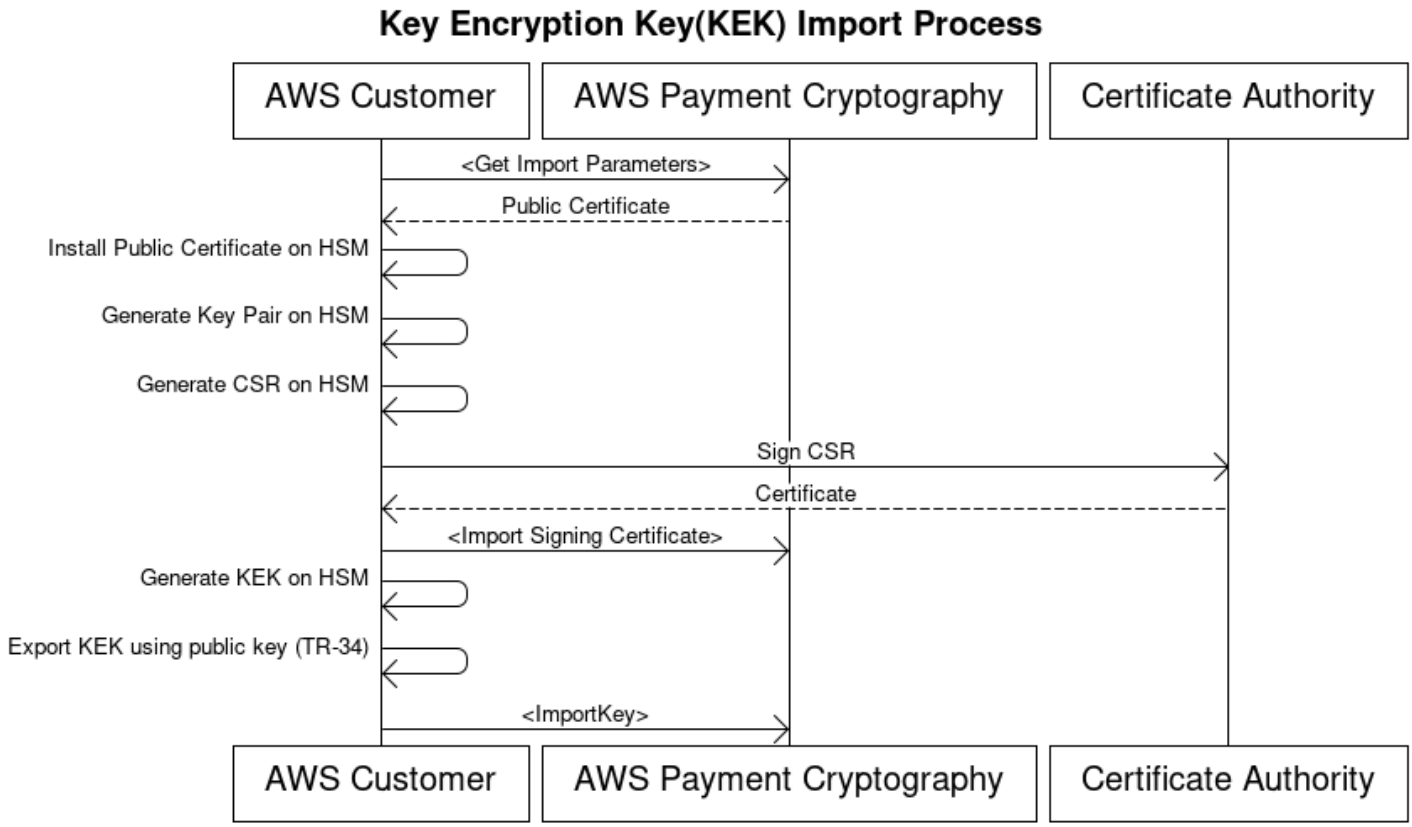
> **Note**
>
> Al importar claves mediante X9.143 bloques de TR-34 claves, la criptografía de AWS pagos normalmente conserva (pero no utiliza) los encabezados opcionales. TR-31 El encabezado HM (tipo hash HMAC) se utiliza durante las operaciones criptográficas. El encabezado KP (KCV de la clave de empaquetado) es específico del proceso de importación y no se conserva.

Cuando se intercambian claves con una contraparte, normalmente se intercambia primero una clave de intercambio de claves (KEK). Esta clave se usará luego para proteger las claves subsiguientes. Al utilizar formatos electrónicos, la KEK se puede intercambiar mediante técnicas asimétricas como TR-34 la envoltura ECDH o RSA. Las claves posteriores se intercambiarán mediante un intercambio de claves simétrico, como. TR-31 Esta KEK tendrá una larga vida útil y solo podrá actualizarse cada pocos años según la política y el período criptográfico definido.

Si solo se intercambian una o dos claves, también puede optar por utilizar técnicas asimétricas para intercambiar directamente esa clave, como un BDK. AWS La criptografía de pagos admite ambos métodos de intercambio de claves.

Importar claves simétricas

Importe claves mediante técnicas asimétricas () TR-34



TR-34 utiliza la criptografía asimétrica RSA para cifrar y firmar claves simétricas para su intercambio. Esto garantiza tanto la confidencialidad (cifrado) como la integridad (firma) de la clave empaquetada.

Para importar tus propias claves, consulta el ejemplo de proyecto AWS de criptografía de pagos en GitHub. Para obtener instrucciones sobre cómo utilizar import/export claves desde otras plataformas, puedes encontrar un ejemplo de código en la guía del usuario de esas plataformas GitHubo consultarla.

1. Ejecute el comando Inicializar la importación

   Llamar a `get-parameters-for-import` para inicializar el proceso de importación. Esta API genera un par de claves para la importación de claves, firma la clave y devuelve el certificado y la raíz del certificado. Cifre la clave que se va a exportar con esta clave. En TR-34 terminología, esto se conoce como certificado KRD. Estos certificados están codificados en base64, son de corta duración y están destinados únicamente a este propósito. Guarde el `ImportToken` valor.

```
$ aws payment-cryptography get-parameters-for-import \
    --key-material-type TR34_KEY_BLOCK \
    --wrapping-key-algorithm RSA_2048
```

```
{
    "ImportToken": "import-token-bwxli6ocftypneu5",
    "ParametersValidUntilTimestamp": 1698245002.065,
    "WrappingKeyCertificateChain": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0....",
    "WrappingKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0....",
    "WrappingKeyAlgorithm": "RSA_2048"
}
```

2. Instale el certificado público en el sistema fuente de claves

   En la mayoría de los HSM, es necesario instalar, cargar o confiar en el certificado público generado en el paso 1 para poder exportar las claves con él. Esto podría incluir toda la cadena de certificados o solo el certificado raíz del paso 1, según el HSM.

3. Genere un par de claves en el sistema fuente y proporcione una cadena de certificados a AWS Payment Cryptography

   Para garantizar la integridad de la carga útil transmitida, la parte que la envía (Key Distribution Host o KDH) la firma. Genere una clave pública para este fin y cree un certificado de clave pública (X509) para devolvérselo a Payment Cryptography. AWS

   Al transferir claves desde un HSM, cree un par de claves en ese HSM. El HSM, un tercero o un servicio similar AWS Private CA pueden generar el certificado.

   Cargue el certificado raíz en AWS Payment Cryptography mediante el `importKey` comando con KeyMaterialType of `RootCertificatePublicKey` y KeyUsageType of. `TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`

   Para los certificados intermedios, utilice el `importKey` comando con KeyMaterialType of `TrustedCertificatePublicKey` y KeyUsageType of`TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`. Repita este proceso para varios certificados intermedios. Utilice el último certificado importado `KeyArn` de la cadena como entrada para los siguientes comandos de importación.

> **Note**
>
> No importe el certificado hoja. Indíquelo directamente durante el comando de importación.

4. Exporte la clave del sistema fuente

   Muchos HSM y sistemas relacionados admiten la exportación de claves utilizando la TR-34 norma. Especifique la clave pública del paso 1 como certificado KRD (de cifrado) y la clave del paso 3 como certificado KDH (de firma). Para importar a AWS Payment Cryptography, especifique el formato como formato de dos pasadas que TR-34.2012 no sea del CMS, que también se puede denominar formato Diebold. TR-34

5. Clave de importación de llamadas

   Llame a la API ImportKey con un KeyMaterialType de`TR34_KEY_BLOCK`. Utilice el keyARN de la última CA importada en el paso 3 para`certificate-authority-public-key-identifier`, el material clave empaquetado del paso 4 para `key-material` y el certificado hoja del paso 3 para. `signing-key-certificate` Incluya el token de importación del paso 1.

```
$ aws payment-cryptography import-key \
    --key-material='{"Tr34KeyBlock": { \
    "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/zabouwe3574jysdl", \
    "ImportToken": "import-token-bwxli6ocftypneu5", \
    "KeyBlockFormat": "X9_TR34_2012", \
    "SigningKeyCertificate":
 "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUV2RENDQXFTZ0F3SUJ...", \
    "WrappedKeyBlock":
 "308205A106092A864886F70D010702A08205923082058E020101310D300B0609608648016503040201308203.
 \
    }'
```

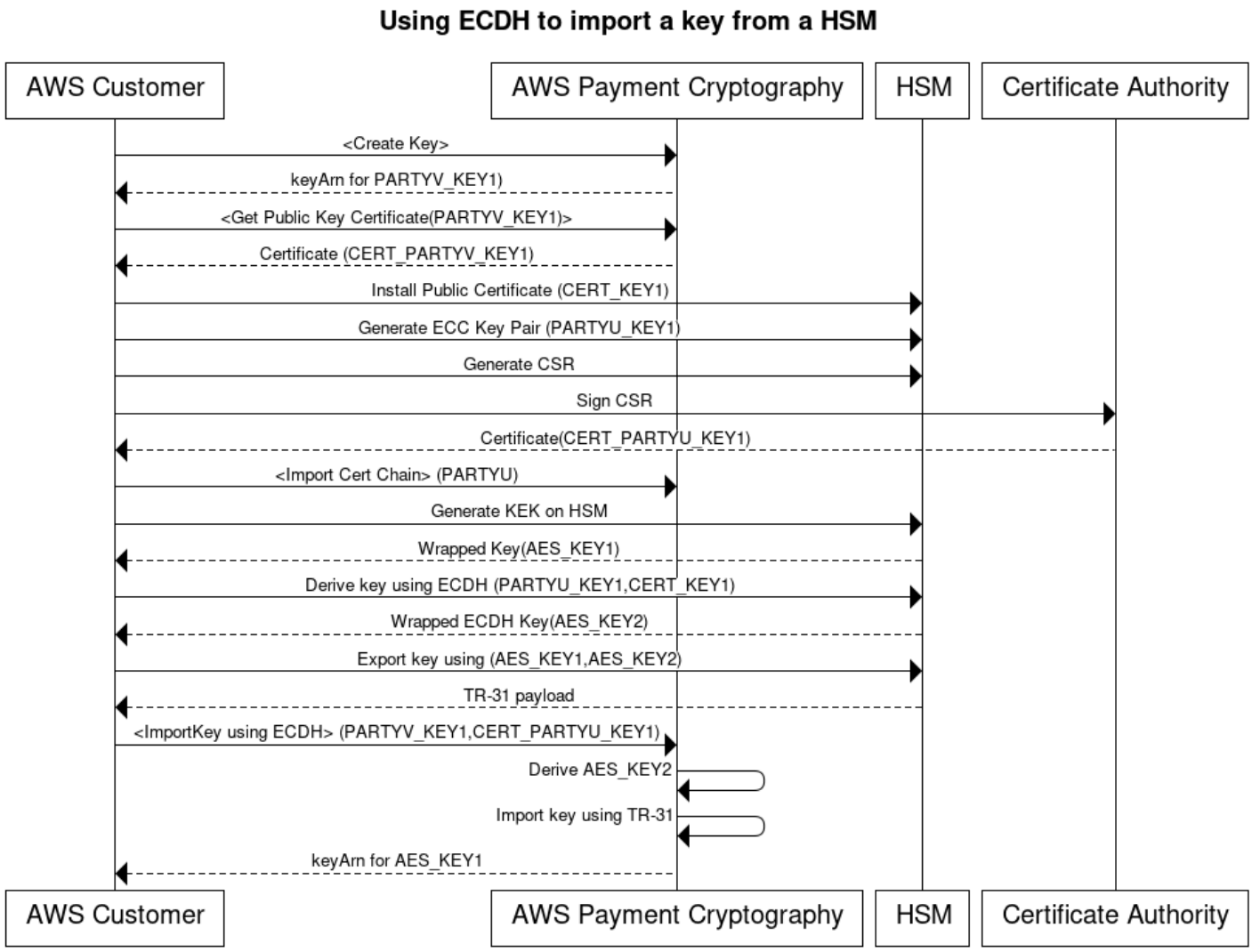
```
{
  "Key": {
    "CreateTimestamp": "2023-06-13T16:52:52.859000-04:00",
    "Enabled": true,
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza",
    "KeyAttributes": {
```

```
      "KeyAlgorithm": "TDES_3KEY",
      "KeyClass": "SYMMETRIC_KEY",
      "KeyModesOfUse": {
        "Decrypt": true,
        "DeriveKey": false,
        "Encrypt": true,
        "Generate": false,
        "NoRestrictions": false,
        "Sign": false,
        "Unwrap": true,
        "Verify": false,
        "Wrap": true
      },
      "KeyUsage": "TR31_K1_KEY_ENCRYPTION_KEY"
    },
    "KeyCheckValue": "CB94A2",
    "KeyCheckValueAlgorithm": "ANSI_X9_24",
    "KeyOrigin": "EXTERNAL",
    "KeyState": "CREATE_COMPLETE",
    "UsageStartTimestamp": "2023-06-13T16:52:52.859000-04:00"
  }
}
```

6. Utilice la clave importada para las operaciones criptográficas o para la importación posterior

   Si la importada KeyUsage era TR31_K0_KEY_ENCRYPTION_KEY, puede usar esta clave para las importaciones de claves posteriores utilizando. TR-31 Para otros tipos de claves (como TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY), puede usar la clave directamente para operaciones criptográficas.

Importe las claves mediante técnicas asimétricas (ECDH)



Elliptic Curve Diffie-Hellman (ECDH) utiliza la criptografía asimétrica ECC para establecer una clave compartida entre dos partes sin necesidad de intercambiar claves previamente. Las claves ECDH son efímeras, por lo que Payment Cryptography no las almacena. AWS En este proceso, se obtiene una única vez mediante el KBPK/KEKECDH. Esa clave derivada se usa inmediatamente para empaquetar la clave real que se desea transferir, que puede ser otra KBPK, una clave IPEK u otro tipo de clave.

Al importar, el sistema de envío se conoce comúnmente como Parte U (iniciadora) y la criptografía de AWS pagos se conoce como Parte V (Responder).

> **Note**
>
> Si bien el ECDH se puede utilizar para intercambiar cualquier tipo de clave simétrica, es el único enfoque que puede transferir claves de forma segura. AES-256

1. Genere un par de claves ECC

   Llame `create-key` para crear un key pair de ECC para este proceso. Esta API genera un par de claves para las importaciones o exportaciones de claves. En el momento de la creación, especifique qué tipo de claves se pueden derivar con esta clave ECC. Cuando utilice el ECDH para intercambiar (empaquetar) otras claves, utilice un valor de. `TR31_K1_KEY_BLOCK_PROTECTION_KEY`

   > **Note**
   >
   > Si bien el ECDH de bajo nivel genera una clave derivada que se puede utilizar para cualquier propósito, la criptografía de AWS pagos limita la reutilización accidental de una clave para varios fines al permitir que una clave solo se utilice para un único tipo de clave derivada.

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=ECC_NIST_P256,KeyUsage=TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT,KeyClass=ASYM
 --derive-key-usage "TR31_K1_KEY_BLOCK_PROTECTION_KEY"
```

```
{
                  "Key": {
                      "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/wc3rjsssguhxtilv",
                      "KeyAttributes": {
                          "KeyUsage": "TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT",
                          "KeyClass": "ASYMMETRIC_KEY_PAIR",
                          "KeyAlgorithm": "ECC_NIST_P256",
                          "KeyModesOfUse": {
                              "Encrypt": false,
                              "Decrypt": false,
                              "Wrap": false,
                              "Unwrap": false,
```

```
                            "Generate": false,
                            "Sign": false,
                            "Verify": false,
                            "DeriveKey": true,
                            "NoRestrictions": false
                        }
                    },
                    "KeyCheckValue": "2432827F",
                    "KeyCheckValueAlgorithm": "CMAC",
                    "Enabled": true,
                    "Exportable": true,
                    "KeyState": "CREATE_COMPLETE",
                    "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                    "CreateTimestamp": "2025-03-28T22:03:41.087000-07:00",
                    "UsageStartTimestamp": "2025-03-28T22:03:41.068000-07:00"
                }
            }
```

2. Obtenga un certificado de clave pública

   Llame `get-public-key-certificate` para recibir la clave pública en forma de X.509 certificado firmado por la entidad emisora de certificados de su cuenta específico para la criptografía de AWS pagos en una región específica.

   Example

```
$ aws payment-cryptography get-public-key-certificate \
                --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/wc3rjsssguhxtilv
```

```
{
            "KeyCertificate": "LS0tLS1CRUdJTi...",
            "KeyCertificateChain": "LS0tLS1CRUdJT..."
      }
```

3. Instale un certificado público en el sistema de contraparte (Parte U)

   En el caso de muchos HSM, es necesario instalar, cargar o confiar en el certificado público generado en el paso 1 para poder exportar las claves con él. Esto podría incluir toda la cadena de certificados o solo el certificado raíz del paso 1, según el HSM. Consulte la documentación del HSM para obtener más información.

4. Genere un par de claves ECC en el sistema de origen y proporcione una cadena de certificados a AWS Payment Cryptography

   En el ECDH, cada parte genera un key pair y acuerda una clave común. Para que la criptografía de AWS pagos pueda obtener la clave, necesita la clave pública de la contraparte en formato de clave X.509 pública.

   Al transferir claves desde un HSM, cree un par de claves en ese HSM. En el caso de los HSM que admiten bloques de teclas, el encabezado de la clave tendrá un aspecto similar a. `D0144K3EX00E0000` Al crear el certificado, por lo general, se genera una CSR en el HSM y, a continuación, en el HSM, un tercero o un servicio que AWS Private CA pueda generar el certificado.

   Cargue el certificado raíz en AWS Payment Cryptography mediante el `importKey` comando of y of. KeyMaterialType `RootCertificatePublicKey` KeyUsageType `TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`

   Para los certificados intermedios, utilice el `importKey` comando con KeyMaterialType of `TrustedCertificatePublicKey` y KeyUsageType of`TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`. Repita este proceso para varios certificados intermedios. Utilice el último certificado importado `KeyArn` de la cadena como entrada para los siguientes comandos de importación.

   > **Note**
   >
   > No importe el certificado hoja. Indíquelo directamente durante el comando de importación.

5. Obtenga la clave de un solo uso mediante el ECDH en el HSM de la Parte U

   Muchos HSM y sistemas relacionados admiten el establecimiento de claves mediante el ECDH. Especifique la clave pública del paso 1 como clave pública y la clave del paso 3 como clave privada. Para ver las opciones permitidas, como los métodos de derivación, consulta la guía de la API.

> **Note**
>
> Los parámetros de derivación, como el tipo de hash, deben coincidir exactamente en ambos lados. De lo contrario, generará una clave diferente.

6. Exporte la clave del sistema fuente

   Por último, exporte la clave que desea transportar a AWS Payment Cryptography mediante TR-31 comandos estándar. Especifique la clave derivada del ECDH como KBPK. La clave que se va a exportar puede ser cualquier clave TDES o AES sujeta a combinaciones TR-31 válidas, siempre que la clave de empaquetado sea al menos tan fuerte como la clave que se va a exportar.

7. Llama a la clave de importación

   Llame a la `import-key` API con un KeyMaterialType de`DiffieHellmanTr31KeyBlock`. Utilice el KeyArn de la última CA importada en el paso 3 `certificate-authority-public-key-identifier` para, el material clave envuelto del paso 4 `key-material` para y el certificado hoja del paso 3 para. `public-key-certificate` Incluya el ARN de clave privada del paso 1.

```
$ aws payment-cryptography import-key \
          --key-material='{
            "DiffieHellmanTr31KeyBlock": {
              "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-
cryptography:us-east-2:111122223333:key/swseahwtq2oj6zi5",
              "DerivationData": {
                "SharedInformation": "1234567890"
              },
              "DeriveKeyAlgorithm": "AES_256",
              "KeyDerivationFunction": "NIST_SP800",
              "KeyDerivationHashAlgorithm": "SHA_256",
              "PrivateKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/wc3rjsssguhxtilv",
              "PublicKeyCertificate":
 "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN....",
              "WrappedKeyBlock":
 "D0112K1TB00E0000D603CCA8ACB71517906600FF8F0F195A38776A7190A0EF0024F088A5342DB98E2735084A7
            }
          }'
```

```
{
        "Key": {
          "CreateTimestamp": "2025-03-13T16:52:52.859000-04:00",
          "Enabled": true,
          "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza",
          "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
              "Decrypt": true,
              "DeriveKey": false,
              "Encrypt": true,
              "Generate": false,
              "NoRestrictions": false,
              "Sign": false,
              "Unwrap": true,
              "Verify": false,
              "Wrap": true
            },
            "KeyUsage": "TR31_K1_KEY_ENCRYPTION_KEY"
          },
          "KeyCheckValue": "CB94A2",
          "KeyCheckValueAlgorithm": "ANSI_X9_24",
          "KeyOrigin": "EXTERNAL",
          "KeyState": "CREATE_COMPLETE",
          "UsageStartTimestamp": "2025-03-13T16:52:52.859000-04:00"
        }
      }
```

8. Utilice la clave importada para las operaciones criptográficas o para la importación posterior

   Si la importada KeyUsage era TR31_K0_KEY_ENCRYPTION_KEY, puede usar esta clave para las importaciones de claves posteriores utilizando. TR-31 Para otros tipos de claves (como TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY), puede usar la clave directamente para operaciones criptográficas.

Importe las claves mediante técnicas asimétricas (RSA Unwrap)

Descripción general: La criptografía AWS de pagos admite RSA wrap/unwrap para el intercambio de claves cuando no es posible. TR-34 Por ejemplo TR-34, esta técnica utiliza la criptografía asimétrica

RSA para cifrar las claves simétricas para su intercambio. Sin embargo, a diferencia de este método TR-34, la parte remitente no firma la carga útil. Además, esta técnica de empaquetado RSA no mantiene la integridad de los metadatos clave durante la transferencia porque no incluye bloques clave.

> **Note**
>
> Puede usar el empaquetado RSA para importar o exportar los TDES y las claves. AES-128

1. Ejecute el comando Inicializar la importación

   Llame get-parameters-for-import para inicializar el proceso de importación con un `KeyMaterialType` de. `KEY_CRYPTOGRAM` `RSA_2048`Utilícelo para el `WrappingKeyAlgorithm` intercambio de claves TDES. Utilice `RSA_3072` o `RSA_4096` cuando intercambie TDES o llaves. AES-128 Esta API genera un par de claves para la importación de claves, firma la clave con una raíz de certificados y devuelve tanto el certificado como la raíz del certificado. Cifre la clave que se va a exportar con esta clave. Estos certificados son de corta duración y están destinados únicamente a este propósito.

   ```
   $ aws payment-cryptography get-parameters-for-import \
       --key-material-type KEY_CRYPTOGRAM \
       --wrapping-key-algorithm RSA_4096
   ```

   ```
   {
     "ImportToken": "import-token-bwxli6ocftypneu5",
     "ParametersValidUntilTimestamp": 1698245002.065,
     "WrappingKeyCertificateChain": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0....",
     "WrappingKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0....",
     "WrappingKeyAlgorithm": "RSA_4096"
   }
   ```

2. Instale el certificado público en el sistema de origen de la clave

   En el caso de muchos HSM, es necesario instalar, cargar o confiar en el certificado público (and/orsu raíz) generado en el paso 1 para poder exportar las claves con él.

3. Exporte la clave del sistema de origen

Muchos HSM y sistemas relacionados admiten la exportación de claves mediante el empaquetado RSA. Especifique la clave pública del paso 1 como certificado de cifrado (). `WrappingKeyCertificate` Si necesita la cadena de confianza, utilice el `WrappingKeyCertificateChain` paso 1. Al exportar la clave desde su HSM, especifique el formato RSA, con el modo de relleno = PKCS #1 v2.2 OAEP (con SHA 256 o SHA 512).

4. Llame import-key

   Llame a la import-key API con un `KeyMaterialType` de`KeyMaterial`. Necesitas el `ImportToken` del paso 1 y el `key-material` (material clave envuelto) del paso 3. Proporcione los parámetros clave (como el uso de claves), ya que el formato RSA no utiliza bloques clave.

```
$ cat import-key-cryptogram.json
```

```
{
  "KeyMaterial": {
    "KeyCryptogram": {
      "Exportable": true,
      "ImportToken": "import-token-bwxli6ocftypneu5",
      "KeyAttributes": {
        "KeyAlgorithm": "AES_128",
        "KeyClass": "SYMMETRIC_KEY",
        "KeyModesOfUse": {
          "Decrypt": true,
          "DeriveKey": false,
          "Encrypt": true,
          "Generate": false,
          "NoRestrictions": false,
          "Sign": false,
          "Unwrap": true,
          "Verify": false,
          "Wrap": true
        },
        "KeyUsage": "TR31_K0_KEY_ENCRYPTION_KEY"
      },
      "WrappedKeyCryptogram": "18874746731....",
      "WrappingSpec": "RSA_OAEP_SHA_256"
    }
  }
}
```

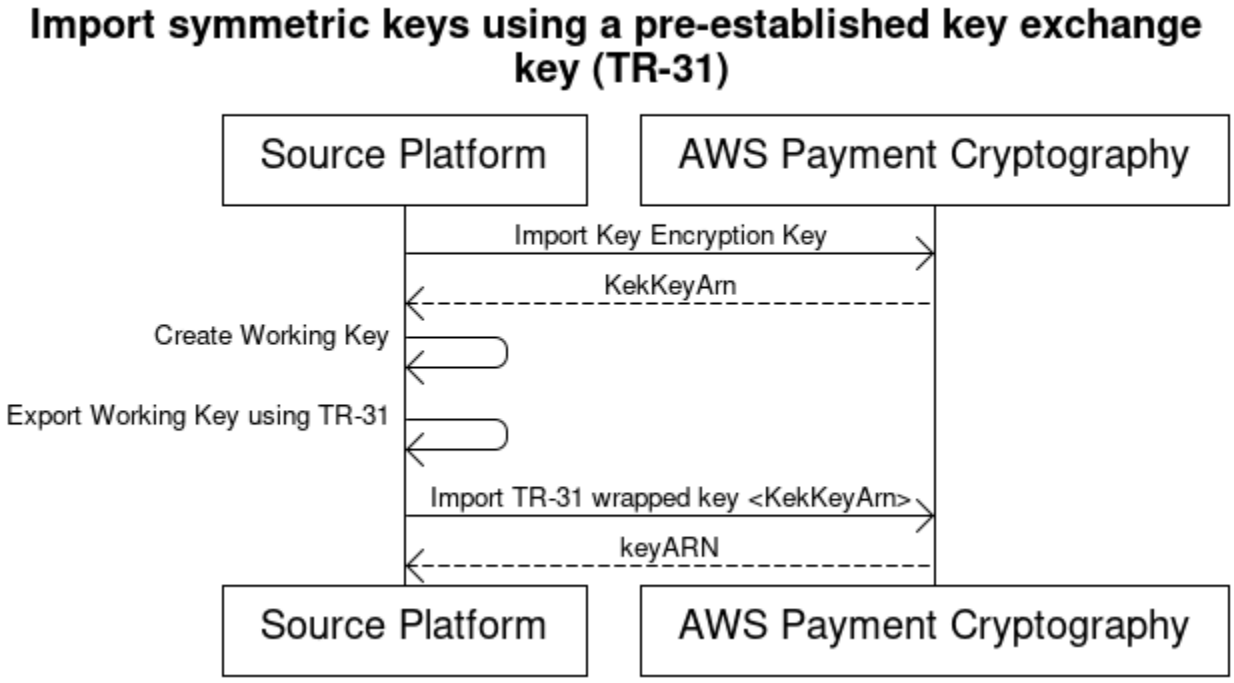
```
$ aws payment-cryptography import-key --cli-input-json file://import-key-
cryptogram.json
```

```
{
  "Key": {
    "KeyOrigin": "EXTERNAL",
    "Exportable": true,
    "KeyCheckValue": "DA1ACF",
    "UsageStartTimestamp": 1697643478.92,
    "Enabled": true,
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
    "CreateTimestamp": 1697643478.92,
    "KeyState": "CREATE_COMPLETE",
    "KeyAttributes": {
      "KeyAlgorithm": "AES_128",
      "KeyModesOfUse": {
        "Encrypt": true,
        "Unwrap": true,
        "Verify": false,
        "DeriveKey": false,
        "Decrypt": true,
        "NoRestrictions": false,
        "Sign": false,
        "Wrap": true,
        "Generate": false
      },
      "KeyUsage": "TR31_K0_KEY_ENCRYPTION_KEY",
      "KeyClass": "SYMMETRIC_KEY"
    },
    "KeyCheckValueAlgorithm": "CMAC"
  }
}
```

5. Utilice la clave importada para las operaciones criptográficas o para la importación posterior

   Si la importada `KeyUsage` fue `TR31_K0_KEY_ENCRYPTION_KEY` o`TR31_K1_KEY_BLOCK_PROTECTION_KEY`, puede usar esta clave para las siguientes importaciones de claves utilizando TR-31. Si el tipo de clave era de cualquier otro tipo (por ejemplo`TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY`), puede utilizarla directamente para operaciones criptográficas.

Importe claves simétricas mediante una clave de intercambio de claves preestablecida () TR-31



Al intercambiar varias claves o permitir la rotación de claves, los socios suelen intercambiar primero una clave de cifrado de clave (KEK) inicial. Puede intercambiar la KEK por la criptografía de AWS pago mediante técnicas como TR-34o. Intercambio de claves físicas

Tras establecer una KEK, puede utilizarla para transportar las claves siguientes (incluidas otras KEK). AWS La criptografía de pagos admite este intercambio de claves mediante el ANSI TR-31, que es ampliamente utilizado y respaldado por los proveedores de HSM.

1. Importar clave: clave de cifrado (KEK)

   Asegúrese de que ya ha importado su KEK y de que tiene el KeyArn (o KeyAlias) disponible.

2. Crea la clave en la plataforma de origen

   Si la clave no existe, créela en la plataforma de origen. Como alternativa, puedes crear la clave en AWS Payment Cryptography y usar el export comando.

3. Exporte la clave desde la plataforma de origen

   Al exportar, especifique el formato de exportación como TR-31. La plataforma de origen solicitará la clave que se va a exportar y la clave de cifrado que se va a utilizar.

4. Importa a AWS Payment Cryptography

Al ejecutar el import-key comando, utilice el keyARN (o alias) de su clave de cifrado para. `WrappingKeyIdentifier` Utilice el resultado de la plataforma de origen para. `WrappedKeyBlock`

Example

```
$ aws payment-cryptography import-key \
    --key-material='{"Tr31KeyBlock": { \
    "WrappingKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ov6icy4ryas4zcza", \
    "WrappedKeyBlock":
 "D0112B0AX00E00002E0A3D58252CB67564853373D1EBCC1E23B2ADE7B15E967CC27B85D5999EF58E11662991F
 \
    }'
```

```
{
  "Key": {
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
    "KeyAttributes": {
      "KeyUsage": "TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY",
      "KeyClass": "SYMMETRIC_KEY",
      "KeyAlgorithm": "AES_128",
      "KeyModesOfUse": {
        "Encrypt": true,
        "Decrypt": true,
        "Wrap": true,
        "Unwrap": true,
        "Generate": false,
        "Sign": false,
        "Verify": false,
        "DeriveKey": false,
        "NoRestrictions": false
      }
    },
    "KeyCheckValue": "0A3674",
    "KeyCheckValueAlgorithm": "CMAC",
    "Enabled": true,
    "Exportable": true,
    "KeyState": "CREATE_COMPLETE",
    "KeyOrigin": "EXTERNAL",
    "CreateTimestamp": "2023-06-02T07:38:14.913000-07:00",
    "UsageStartTimestamp": "2023-06-02T07:38:14.857000-07:00"
  }
}
```

Importación de claves públicas asimétricas (RSA, ECC)

Todos los certificados importados deben ser al menos tan seguros como el certificado de emisión (predecesor) de la cadena. Esto significa que un RSA_2048 CA solo se puede utilizar para proteger un certificado base RSA_2048 y que un certificado ECC debe estar protegido por otro certificado ECC de solidez equivalente. Un certificado ECC P384 solo puede emitirlo una CA P384 o P521. Todos los certificados no deben estar vencidos en el momento de la importación.

Importar claves públicas RSA

AWS La criptografía de pagos admite la importación de claves RSA públicas como certificados. X.509 Para importar un certificado, primero importe su certificado raíz. Todos los certificados deben estar vigentes en el momento de la importación. El certificado debe estar en formato PEM y estar codificado en base64.

1. Importe el certificado raíz a la criptografía de pagos AWS

   Utilice el siguiente comando para importar el certificado raíz:

Example

2. Importe el certificado de clave pública a la criptografía AWS de pagos

   Ahora puede importar una clave pública. Como TR-34 el ECDH se basa en la emisión del certificado principal en tiempo de ejecución, esta opción solo se utiliza cuando se cifran datos con una clave pública de otro sistema. KeyUsage se establecerá en TR31_D1_ASYMMETRIC_KEY_FOR_DATA_ENCRYPTION.

Example

```
$ aws payment-cryptography import-key \
    --key-material='{"Tr31KeyBlock": { \
    "WrappingKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ov6icy4ryas4zcza", \
    "WrappedKeyBlock":
 "D0112B0AX00E00002E0A3D58252CB67564853373D1EBCC1E23B2ADE7B15E967CC27B85D5999EF58E11662991F
 \
    }'
```

```
{
  "Key": {
    "CreateTimestamp": "2023-08-08T18:55:46.815000+00:00",
    "Enabled": true,
    "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/4kd6xud22e64wcbk",
    "KeyAttributes": {
      "KeyAlgorithm": "RSA_4096",
      "KeyClass": "PUBLIC_KEY",
      "KeyModesOfUse": {
        "Decrypt": false,
        "DeriveKey": false,
        "Encrypt": false,
        "Generate": false,
        "NoRestrictions": false,
        "Sign": false,
        "Unwrap": false,
        "Verify": true,
        "Wrap": false
      },
      "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE"
    },
    "KeyOrigin": "EXTERNAL",
    "KeyState": "CREATE_COMPLETE",
    "UsageStartTimestamp": "2023-08-08T18:55:46.815000+00:00"
  }
}
```

Importación de claves públicas ECC

AWS La criptografía de pagos admite la importación de claves ECC públicas como certificados. X.509 Para importar un certificado, importe primero su certificado CA raíz y cualquier certificado intermedio. Todos los certificados deben estar vigentes en el momento de la importación. El certificado debe estar en formato PEM y estar codificado en base64.

1. Importe el certificado raíz ECC a la criptografía de pagos AWS

   Utilice el siguiente comando para importar el certificado raíz:

Example

2. Importe el certificado intermedio a la criptografía AWS de pagos

   Utilice el siguiente comando para importar un certificado intermedio:

Example

3. Importe un certificado de clave pública (Leaf) a la criptografía AWS de pagos

   Si bien se puede importar un certificado ECC estándar, actualmente no hay funciones definidas en la criptografía de AWS pagos para este certificado además del almacenamiento. Esto se debe a que, cuando se utilizan funciones ECDH, el certificado hoja se transfiere en tiempo de ejecución.

Exportar claves

Contenido

- Exporta claves simétricas
  - Exporte las claves mediante técnicas asimétricas () TR-34
  - Exporte las claves mediante técnicas asimétricas (ECDH)
  - Exporte las claves mediante técnicas asimétricas (RSA Wrap)
  - Exporte claves simétricas mediante una clave de intercambio de claves preestablecida () TR-31
- Exporte las claves iniciales de DUKPT () IPEK/IK
- Especifique los encabezados de los bloques clave para la exportación
  - Cabeceras comunes
- Exporte claves asimétricas (RSA)

Exporta claves simétricas

> **Important**
>
> Asegúrese de tener la última versión de AWS CLI antes de empezar. Para actualizar, consulte Instalación del AWS CLI.

Exporte las claves mediante técnicas asimétricas () TR-34

TR-34 utiliza la criptografía asimétrica RSA para cifrar y firmar claves simétricas para su intercambio. El cifrado protege la confidencialidad, mientras que la firma garantiza la integridad. Al exportar las claves, la criptografía de AWS pagos actúa como el host de distribución de claves (KDH) y el sistema de destino se convierte en el dispositivo receptor de claves (KRD).

> **Note**
>
> Si su HSM admite la TR-34 exportación pero no la TR-34 importación, le recomendamos que primero establezca una KEK compartida entre su HSM y la criptografía de pagos mediante. AWS TR-34 A continuación, puede utilizarla TR-31 para transferir el resto de las claves.

1. Inicializa el proceso de exportación

   Ejecute get-parameters-for-export para generar un par de claves para la exportación de claves. Usamos este par de claves para firmar la TR-34 carga útil. En TR-34 terminología, este es el certificado de firma de KDH. Los certificados son de corta duración y solo son válidos durante el período especificado en. `ParametersValidUntilTimestamp`

   > **Note**
   >
   > Todos los certificados están codificados en base64.

   Example

   ```
   $ aws payment-cryptography get-parameters-for-export \
       --signing-key-algorithm RSA_2048 \
       --key-material-type TR34_KEY_BLOCK
   ```

   ```
   {
     "SigningKeyCertificate":
    "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUV2RENDQXFTZ0F3SUJ...",
     "SigningKeyCertificateChain": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS....",
     "SigningKeyAlgorithm": "RSA_2048",
     "ExportToken": "export-token-au7pvkbsq4mbup6i",
     "ParametersValidUntilTimestamp": "2023-06-13T15:40:24.036000-07:00"
   }
   ```

2. Importe el certificado AWS de criptografía de pago a su sistema receptor

   Importe la cadena de certificados del paso 1 a su sistema de recepción.

3. Configure los certificados de su sistema de recepción

Para proteger la carga útil transmitida, la parte emisora (KDH) la cifra. Su sistema receptor (normalmente su HSM o el HSM de su socio) necesita generar una clave pública y crear un certificado de clave pública. X.509 Puede usarlo AWS Private CA para generar certificados, pero puede usar cualquier autoridad de certificación.

Una vez que tenga el certificado, importe el certificado raíz a AWS Payment Cryptography mediante el ImportKey comando. Establezca `KeyMaterialType` en `RootCertificatePublicKey` y `KeyUsageType` en `TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`.

Lo usamos `TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE` como la `KeyUsageType` porque es la clave raíz que firma el certificado hoja. No necesitas importar los certificados hoja a AWS Payment Cryptography; puedes pasarlos por Internet.

> **Note**
>
> Si importó anteriormente el certificado raíz, omita este paso. Para los certificados intermedios, utilice`TrustedCertificatePublicKey`.

4. Exporte su clave

   Llama a la ExportKey API con `KeyMaterialType` set to`TR34_KEY_BLOCK`. Debes proporcionar:

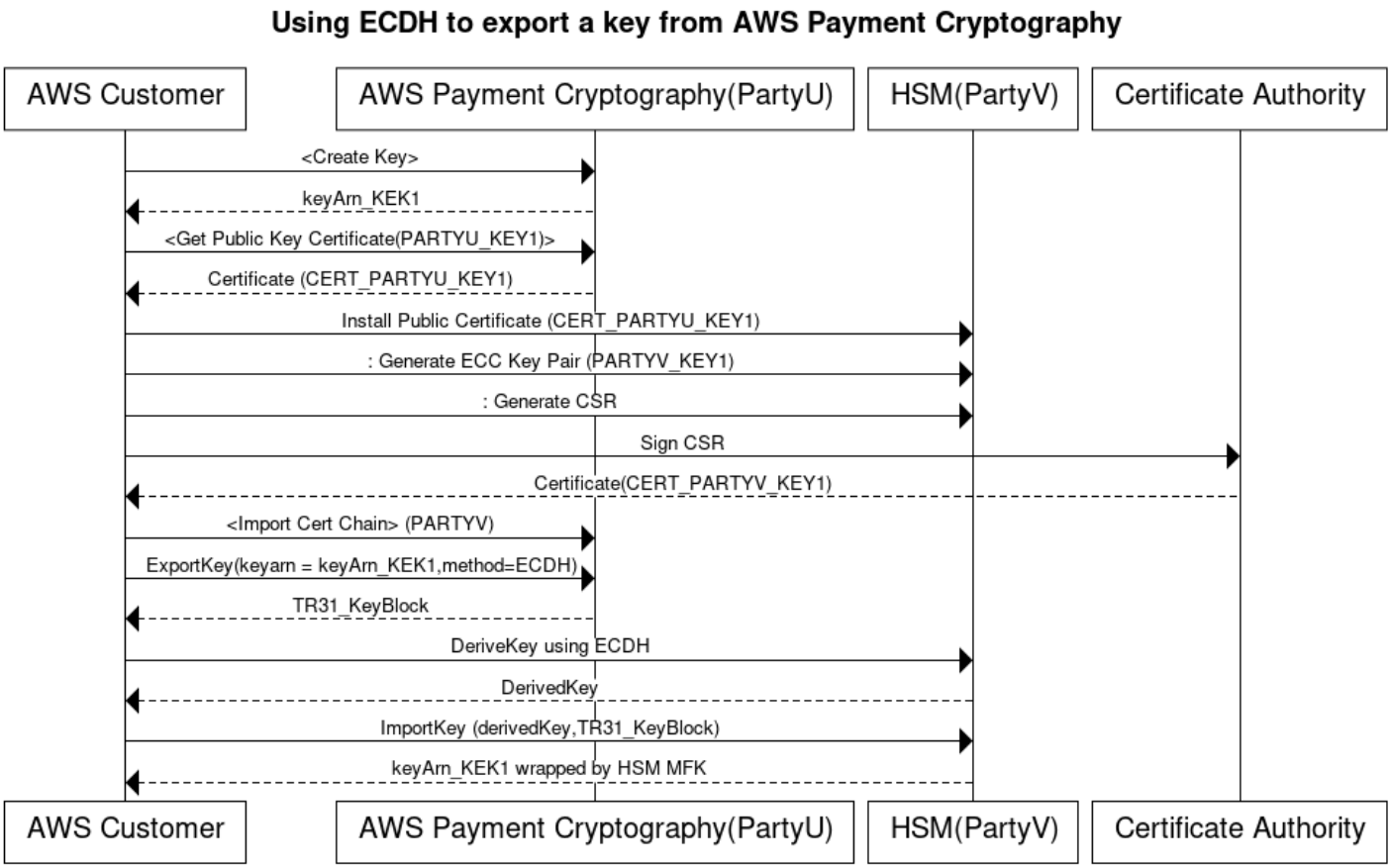
   - El keyArn de la CA raíz del paso 3 como `CertificateAuthorityPublicKeyIdentifier`
   - El certificado hoja del paso 3 es `WrappingKeyCertificate`
   - El keyARN (o alias) de la clave que desea exportar como `--export-key-identifier`
   - El token de exportación del paso 1

Example

```
$ aws payment-cryptography export-key \
    --export-key-identifier "example-export-key" \
    --key-material '{"Tr34KeyBlock": { \
    "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/4kd6xud22e64wcbk", \
    "ExportToken": "export-token-au7pvkbsq4mbup6i", \
    "KeyBlockFormat": "X9_TR34_2012", \
    "WrappingKeyCertificate":
 "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUV2RENDQXFXZ0F3SUJBZ0lSQ..."} \
    }'
```

```
{
  "WrappedKey": {
    "KeyMaterial": "308205A106092A864886F70D010702A08205923082058...",
    "WrappedKeyMaterialFormat": "TR34_KEY_BLOCK"
  }
}
```

Exporte las claves mediante técnicas asimétricas (ECDH)



Elliptic Curve Diffie-Hellman (ECDH) utiliza la criptografía asimétrica ECC para establecer una clave compartida entre dos partes sin necesidad de intercambiar claves previamente. Las claves ECDH son efímeras, por lo que Payment Cryptography no las almacena. AWS En este proceso, se obtiene una única vez mediante el KBPK/KEKECDH. Esa clave derivada se usa inmediatamente para empaquetar la clave que se desea transferir, que puede ser otra clave KBPK, BDK, IPEK u otro tipo de clave.

Al exportar, la criptografía de AWS pagos se denomina Parte U (iniciadora) y el sistema receptor se denomina Parte V (Responder).

> **Note**
>
> El ECDH se puede utilizar para intercambiar cualquier tipo de clave simétrica, pero es el único enfoque que se puede utilizar para transferir AES-256 claves si aún no se ha establecido una KEK.

1. Genere un par de claves ECC

   Llame `create-key` para crear un key pair de ECC para este proceso. Esta API genera un par de claves para las importaciones o exportaciones de claves. En el momento de la creación, especifique qué tipo de claves se pueden derivar con esta clave ECC. Cuando utilice el ECDH para intercambiar (empaquetar) otras claves, utilice un valor de. `TR31_K1_KEY_BLOCK_PROTECTION_KEY`

   > **Note**
   >
   > Si bien el ECDH de bajo nivel genera una clave derivada que se puede utilizar para cualquier propósito, la criptografía de AWS pagos limita la reutilización accidental de una clave para varios fines al permitir que una clave solo se utilice para un único tipo de clave derivada.

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=ECC_NIST_P256,KeyUsage=TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT,KeyClass=ASYM
 --derive-key-usage "TR31_K1_KEY_BLOCK_PROTECTION_KEY"
```

```
{
        "Key": {
            "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
wc3rjsssguhxtilv",
            "KeyAttributes": {
                "KeyUsage": "TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT",
                "KeyClass": "ASYMMETRIC_KEY_PAIR",
                "KeyAlgorithm": "ECC_NIST_P256",
                "KeyModesOfUse": {
                    "Encrypt": false,
                    "Decrypt": false,
                    "Wrap": false,
                    "Unwrap": false,
                    "Generate": false,
                    "Sign": false,
                    "Verify": false,
                    "DeriveKey": true,
                    "NoRestrictions": false
                }
            },
```

```
            "KeyCheckValue": "2432827F",
            "KeyCheckValueAlgorithm": "CMAC",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2025-03-28T22:03:41.087000-07:00",
            "UsageStartTimestamp": "2025-03-28T22:03:41.068000-07:00"
        }
    }
```

2. Obtenga un certificado de clave pública

   Llame `get-public-key-certificate` para recibir la clave pública en forma de X.509 certificado firmado por la entidad emisora de certificados de su cuenta específico para la criptografía de AWS pagos en una región específica.

   Example

```
$ aws payment-cryptography get-public-key-certificate \
          --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/wc3rjsssguhxtilv
```

```
{
      "KeyCertificate": "LS0tLS1CRUdJTi...",
      "KeyCertificateChain": "LS0tLS1CRUdJT..."
    }
```

3. Instale un certificado público en el sistema de contraparte (Parte V)

   Con muchos HSM, es necesario instalar, cargar o confiar en el certificado público generado en el paso 1 para establecer las claves. Esto podría incluir toda la cadena de certificados o solo el certificado raíz, según el HSM. Consulte la documentación del HSM para obtener instrucciones específicas.

4. Genere un par de claves ECC en el sistema de origen y proporcione una cadena de certificados a AWS Payment Cryptography

   En el ECDH, cada parte genera un key pair y acuerda una clave común. Para que la criptografía de AWS pagos pueda obtener la clave, necesita la clave pública de la contraparte en formato de clave X.509 pública.

Al transferir claves desde un HSM, cree un par de claves en ese HSM. En el caso de los HSM que admiten bloques de teclas, el encabezado de la clave tendrá un aspecto similar a. `D0144K3EX00E0000` Al crear el certificado, normalmente se genera una CSR en el HSM y, a continuación, el HSM, un tercero o un servicio como el que AWS Private CA pueda generar el certificado.

Cargue el certificado raíz en AWS Payment Cryptography mediante el `importKey` comando of y of. KeyMaterialType `RootCertificatePublicKey` KeyUsageType `TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`

Para los certificados intermedios, utilice el `importKey` comando con KeyMaterialType of `TrustedCertificatePublicKey` y KeyUsageType of`TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE`. Repita este proceso para varios certificados intermedios. Utilice el último certificado importado `KeyArn` de la cadena como entrada para los siguientes comandos de exportación.

> **Note**
>
> No importe el certificado hoja. Indíquelo directamente durante el comando de exportación.

5. Obtenga la clave y exporte la clave de la criptografía de AWS pagos

Al exportar, el servicio obtiene una clave mediante el ECDH y, a continuación, la utiliza inmediatamente como KBPK para empaquetar la clave y exportarla. TR-31 La clave que se va a exportar puede ser cualquier clave TDES o AES sujeta a combinaciones TR-31 válidas, siempre que la clave de empaquetado sea al menos tan fuerte como la clave que se va a exportar.

```
$ aws payment-cryptography export-key \
            --export-key-identifier arn:aws:payment-cryptography:us-
west-2:529027455495:key/e3a65davqhbpjm4h \
            --key-material='{
              "DiffieHellmanTr31KeyBlock": {
                "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-
cryptography:us-east-2:111122223333:key/swseahwtq2oj6zi5",
                "DerivationData": {
                  "SharedInformation": "ADEF567890"
                },
                "DeriveKeyAlgorithm": "AES_256",
```

```
                "KeyDerivationFunction": "NIST_SP800",
                "KeyDerivationHashAlgorithm": "SHA_256",
                "PrivateKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/wc3rjsssguhxtilv",
                "PublicKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FUR..."
              }
            }'
```

```
{
            "WrappedKey": {
                "WrappedKeyMaterialFormat": "TR31_KEY_BLOCK",
                "KeyMaterial":
 "D0112K1TB00E00007012724C0FAAF64DA50E2FF4F9A94DF50441143294E0E995DB2171554223EAA56D078C4CF
                "KeyCheckValue": "E421AD",
                "KeyCheckValueAlgorithm": "ANSI_X9_24"
            }
        }
```

6. Obtenga la clave de un solo uso mediante el ECDH en el HSM de la Parte V

   Muchos HSM y sistemas relacionados admiten el establecimiento de claves mediante el ECDH. Especifique la clave pública del paso 1 como clave pública y la clave del paso 3 como clave privada. Para ver las opciones permitidas, como los métodos de derivación, consulta la guía de la API.

   > **Note**
   >
   > Los parámetros de derivación, como el tipo de hash, deben coincidir exactamente en ambos lados. De lo contrario, generará una clave diferente.

7. Importe la clave al sistema de destino

   Por último, importe la clave de AWS Payment Cryptography mediante TR-31 comandos estándar. Especifique la clave derivada del ECDH como KBPK y utilice el bloque de TR-31 claves que se exportó anteriormente desde Payment Cryptography. AWS

Exporte las claves mediante técnicas asimétricas (RSA Wrap)

Cuando TR-34 no esté disponible, puede usar RSA wrap/unwrap para el intercambio de claves. Por ejemplo TR-34, este método utiliza la criptografía asimétrica RSA para cifrar las claves simétricas. Sin embargo, la envoltura RSA no incluye:

- Firma de la carga útil por parte de la parte remitente
- Bloques clave que mantienen la integridad de los metadatos clave durante el transporte

> **Note**
>
> Puede utilizar el empaquetado RSA para exportar los TDES y AES-128 las claves.

1. Cree una clave y un certificado RSA en su sistema de recepción

   Cree o identifique una clave RSA para recibir la clave empaquetada. Requerimos que las claves estén en formato X.509 de certificado. Asegúrese de que el certificado esté firmado por un certificado raíz que pueda importar a AWS Payment Cryptography.
2. Importe el certificado público raíz a AWS Payment Cryptography

   import-keyUtilícelo con la `--key-material` opción de importar el certificado

```
$ aws payment-cryptography import-key \
    --key-material='{"RootCertificatePublicKey": { \
    "KeyAttributes": { \
    "KeyAlgorithm": "RSA_4096", \
    "KeyClass": "PUBLIC_KEY", \
    "KeyModesOfUse": {"Verify": true}, \
    "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE"}, \
    "PublicKeyCertificate": "LS0tLS1CRUdJTiBDRV..."} \
    }'
```

```
{
  "Key": {
    "CreateTimestamp": "2023-09-14T10:50:32.365000-07:00",
    "Enabled": true,
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
nsq2i3mbg6sn775f",
    "KeyAttributes": {
```

```
      "KeyAlgorithm": "RSA_4096",
      "KeyClass": "PUBLIC_KEY",
      "KeyModesOfUse": {
        "Decrypt": false,
        "DeriveKey": false,
        "Encrypt": false,
        "Generate": false,
        "NoRestrictions": false,
        "Sign": false,
        "Unwrap": false,
        "Verify": true,
        "Wrap": false
      },
      "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE"
    },
    "KeyOrigin": "EXTERNAL",
    "KeyState": "CREATE_COMPLETE",
    "UsageStartTimestamp": "2023-09-14T10:50:32.365000-07:00"
  }
}
```

3. Exporta tu clave

   Dígale a AWS Payment Cryptography que exporte su clave con su certificado principal. Debe especificar:

   - El ARN del certificado raíz que importó en el paso 2
   - El certificado foliar para la exportación
   - La clave simétrica para exportar

   El resultado es una versión empaquetada (cifrada) binaria codificada en hexadecimal de la clave simétrica.

Example Ejemplo: exportar una clave

```
$ cat export-key.json
```

```
{
  "ExportKeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
  "KeyMaterial": {
    "KeyCryptogram": {
      "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/zabouwe3574jysdl",
      "WrappingKeyCertificate": "LS0tLS1CRUdJTiBDEXAMPLE...",
      "WrappingSpec": "RSA_OAEP_SHA_256"
    }
  }
}
```

```
$ aws payment-cryptography export-key \
    --cli-input-json file://export-key.json
```

```
{
  "WrappedKey": {
    "KeyMaterial":
 "18874746731E9E1C4562E4116D1C2477063FCB08454D757D81854AEAEE0A52B1F9D303FA29C02DC82AE778535
    "WrappedKeyMaterialFormat": "KEY_CRYPTOGRAM"
  }
}
```

4. Importe la clave a su sistema de recepción

   Muchos HSM y sistemas relacionados admiten la importación de claves mediante RSA unwrap (incluida la criptografía de AWS pagos). Al importar, especifique:

   - La clave pública del paso 1 como certificado de cifrado
   - El formato es RSA
   - Modo de relleno como PKCS #1 v2.2 OAEP (con SHA 256)

> **Note**
>
> Generamos la clave empaquetada en formato HexBinary. Es posible que necesite convertir el formato si su sistema requiere una representación binaria diferente, como base64.

Exporte claves simétricas mediante una clave de intercambio de claves preestablecida () TR-31

Al intercambiar varias claves o permitir la rotación de claves, los socios suelen intercambiar primero una clave de cifrado de clave (KEK) inicial. Puede intercambiar la KEK por la criptografía de AWS pago mediante técnicas como TR-34o. Intercambio de claves físicas Tras establecer una KEK, puede utilizarla para transportar las claves siguientes, incluidas otras KEK. Apoyamos este intercambio de claves mediante ANSI TR-31, que es ampliamente compatible con los proveedores de HSM.

1. Configure su clave de cifrado de claves (KEK)

   Asegúrese de que ya ha intercambiado su KEK y de que tiene el KeyArn (o KeyAlias) disponible.

2. Crea tu clave en criptografía de pagos AWS

   Crea tu clave si aún no existe. Como alternativa, puedes crear la clave en el otro sistema y usar el comando de importación.

3. Exporta tu clave desde AWS Payment Cryptography

   Al exportar en TR-31 formato, especifique la clave que desee exportar y la clave de empaquetado que desee utilizar.

Example Ejemplo: exportar una clave con el bloque de teclas TR31

```
$ aws payment-cryptography export-key \
    --key-material='{"Tr31KeyBlock": \
    { "WrappingKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ov6icy4ryas4zcza" }}' \
    --export-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/5rplquuwozodpwsp
```

```
{
  "WrappedKey": {
    "KeyCheckValue": "73C263",
    "KeyCheckValueAlgorithm": "ANSI_X9_24",
    "KeyMaterial":
 "D0144K0AB00E0000A24D3ACF3005F30A6E31D533E07F2E1B17A2A003B338B1E79E5B3AD4FBF7850FACF9A3784
    "WrappedKeyMaterialFormat": "TR31_KEY_BLOCK"
  }
}
```

4. Importe la clave a su sistema

   Utilice la implementación de clave de importación de su sistema para importar la clave.

Exporte las claves iniciales de DUKPT () IPEK/IK

Al utilizar DUKPT, puede generar una única clave de derivación base (BDK) para una flota de terminales. Los terminales no tienen acceso directo al BDK. En su lugar, cada terminal recibe una clave de terminal inicial única, conocida como IPEK o clave inicial (IK). Cada IPEK se deriva del BDK mediante un número de serie clave (KSN) único.

La estructura de KSN varía según el tipo de cifrado:

- Para el TDES: el KSN de 10 bytes incluye:
  - 24 bits para el ID del conjunto de claves
  - 19 bits para el ID del terminal
  - 21 bits para el contador de transacciones
- Para el AES: el KSN de 12 bytes incluye:
  - 32 bits para el ID de BDK

- 32 bits para el identificador de derivación (ID)
- 32 bits para el contador de transacciones

Proporcionamos un mecanismo para generar y exportar estas claves iniciales. Puede exportar las claves generadas mediante TR-31 los métodos de TR-34 empaquetado RSA o RSA. Tenga en cuenta que las claves IPEK no se conservan y no se pueden usar para operaciones posteriores con la criptografía de pagos. AWS

No imponemos la división entre las dos primeras partes de la KSN. Si desea almacenar el identificador de derivación con el BDK, puede utilizar etiquetas. AWS

> **Note**
>
> La parte del contador del KSN (32 bits para el AES DUKPT) no se utiliza para la derivación. IPEK/IK Por ejemplo, las entradas 12345678901234560001 y 12345678901234569999 generarán el mismo IPEK.

```
$ aws payment-cryptography export-key \
    --key-material='{"Tr31KeyBlock": { \
    "WrappingKeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza"}} ' \
    --export-key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
    --export-attributes 'ExportDukptInitialKey={KeySerialNumber=12345678901234560001}'
```

```
{
"WrappedKey": {
    "KeyCheckValue": "73C263",
    "KeyCheckValueAlgorithm": "ANSI_X9_24",
    "KeyMaterial":
 "B0096B1TX00S000038A8A06588B9011F0D5EEF1CCAECFA6962647A89195B7A98BDA65DDE7C57FEA507559AF2A5D60
    "WrappedKeyMaterialFormat": "TR31_KEY_BLOCK"
}
}
```

Especifique los encabezados de los bloques clave para la exportación

Puede modificar o añadir la información de los bloques clave al exportar en ASC o en formatos TR-31 . TR-34 En la siguiente tabla se describe el formato de los bloques de TR-31 teclas y los elementos que se pueden modificar durante la exportación.

Atributo del bloque clave	Finalidad	¿Se puede modificar durante la exportación?	Notas
ID de versión.	Define el método utilizado para proteger el material clave. La norma incluye: • Versiones A y C (variante clave, obsoleta) • Versión B (derivación mediante TDES) • Versión D (derivación de claves mediante AES)	No	Usamos la versión B para las claves de empaquetado TDES y la versión D para las claves de empaquetado AES. Solo admitimos las versiones A y C para las operaciones de importación.
Longitud del bloque de claves	Especifica la longitud del mensaje restante	No	Calculamos este valor automáticamente. La longitud puede parecer incorrecta antes de descifrar la carga útil, ya que podemos añadir un relleno de teclas según lo exija la especificación.

Atributo del bloque clave	Finalidad	¿Se puede modificar durante la exportación?	Notas
Uso de claves	Define los fines permitidos para la clave, como: • C0 (verificación de tarjetas) • B0 (clave de derivación básica)	No	
Algoritmo	Especifica el algoritmo de la clave subyacente. Apoyamos: • (TDES) • H (HMAC) • A (AES)	No	Exportamos este valor tal cual.
Uso de claves	Define las operaciones permitidas, como: • Generar y verificar (C) • Encrypt/Decrypt/Wrap/Unwrap (B)	Sí*	
Versión clave	Indica el número de versión de la clave replacement/rotation. El valor predeterminado es 00 si no se especifica.	Sí, se puede añadir	

Atributo del bloque clave	Finalidad	¿Se puede modificar durante la exportación?	Notas
Exportabilidad clave	Controla si la clave se puede exportar: • N: no es exportable • E: Exporta según X9.24 (bloques clave) • S - Exportar en formatos de bloques clave o sin bloques clave	Sí*	
Bloques clave opcionales	Sí, se puede adjuntar	Los bloques de claves opcionales son name/value pares enlazados criptográficamente a la clave. Por ejemplo, el KeySet ID de las claves DUKPT. Calculamos automáticamente el número de bloques, la longitud de cada bloque y el bloque de relleno (PB) en función del par introducido. name/value	

*Al modificar los valores, el nuevo valor debe ser más restrictivo que el valor actual en la criptografía de AWS pagos. Por ejemplo:

- Si el modo de uso clave actual es Generate=True, Verify=True, puede cambiarlo a Generate=True, Verify=False
- Si la clave ya está configurada como no exportable, no puedes cambiarla a exportable

Al exportar claves, aplicamos automáticamente los valores actuales de la clave que se está exportando. Sin embargo, es posible que desee modificar o añadir esos valores antes de enviarlos al sistema receptor. Estos son algunos de los escenarios más comunes:

- Al exportar una clave a un terminal de pago, defina su exportabilidad en `Not Exportable` porque los terminales normalmente solo importan claves y no deberían exportarlas.
- Cuando necesites pasar los metadatos clave asociados al sistema receptor, usa encabezados TR-31 opcionales para vincular criptográficamente los metadatos a la clave en lugar de crear una carga personalizada.
- Defina la versión de la clave mediante el `KeyVersion` campo para realizar un seguimiento de la rotación de la clave.

TR-31/X9.143 define encabezados comunes, pero puede usar otros encabezados siempre que cumplan con los parámetros de criptografía de AWS pagos y su sistema receptor pueda aceptarlos. Para obtener más información sobre los encabezados de los bloques clave durante la exportación, consulte los encabezados de los bloques clave en la Guía de la API.

Este es un ejemplo de exportación de una clave BDK (por ejemplo, a un KIF) con estas especificaciones:

- Versión clave: 02
- KeyExportability: NON_EXPORTABLE
- KeySetID: 00ABCDEFAB (00 indica la clave TDES, ABCDEFABCD es la clave inicial)

Como no especificamos los modos de uso clave, esta clave hereda el modo de uso de arn:aws:payment-cryptography:us-east- 2:111122223333: (= true). key/5rplquuwozodpwsp DeriveKey

> **Note**
>
> Incluso si en este ejemplo estableces la exportabilidad como No exportable, el KIF aún puede:

- Derive claves como las que se utilizan en IPEK/IKDUKPT
- Exporte estas claves derivadas para instalarlas en los dispositivos

Esto lo permiten específicamente las normas.

```
$ aws payment-cryptography export-key \
    --key-material='{"Tr31KeyBlock": { \
    "WrappingKeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza", \
    "KeyBlockHeaders": { \
    "KeyModesOfUse": { \
    "Derive": true}, \
    "KeyExportability": "NON_EXPORTABLE", \
    "KeyVersion": "02", \
    "OptionalBlocks": { \
    "BI": "00ABCDEFABCD"}}} \
    }' \
    --export-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/5rplquuwozodpwsp
```

```
{
"WrappedKey": {
    "WrappedKeyMaterialFormat": "TR31_KEY_BLOCK",
    "KeyMaterial": "EXAMPLE_KEY_MATERIAL_TR31",
    "KeyCheckValue": "A4C9B3",
    "KeyCheckValueAlgorithm": "ANSI_X9_24"
    }
}
```

Cabeceras comunes

X9.143 define ciertos encabezados para casos de uso comunes. Con la excepción del encabezado HM (HMAC Hash), AWS Payment Cryptography no analiza ni utiliza estos encabezados.

Nombre del encabezado	Finalidad	Validación típica	Notas
BI	Identificador de clave de derivación base para DUKPT	2 caracteres hexadecimales (00 para TDES, 11 para AES) y 10 caracteres hexadecimales para TDES KSI u 8 caracteres hexadecimales para BDK ID (AES DUKPT).	Contiene el (BDK ID, para AES DUKPT) o el identificador del conjunto de claves (KSI, para TDES DUKPT). Se puede utilizar para intercambiar el ID del BDK o el KSI, pero no es necesario intercambiar los demás datos contenidos en los bloques IK y KS. Normalmente, el BI se utiliza cuando se transmite a un KIF, mientras que el IK o el KS se utilizan cuando se inyecta en el propio terminal.
HM	Especifica el tipo de hash para las operaciones de HMAC	• 10 — SHA-1 • 20 — SHA-224 • 21 — SHA-256 • 22 — SHA-384 • 23 — SHA-512 • 24 — SHA-512/224 • 25 — SHA-512/256 • 30 — SHA3-224 • 31 — SHA3-256 • 32 — SHA3-384	El servicio rellena automáticamente este campo al exportar y lo analizará al importarlo. Los tipos de hash que no admite el servicio, como SHAKE128, se pueden importar, pero es posible que no se puedan utilizar para

Nombre del encabezado	Finalidad	Validación típica	Notas
		• 33 — SHA3-512 • 40 — SHAKE128 • 41 — SHAKE256	funciones criptográficas.
IK	Número de serie de la clave inicial para AES DUKPT	16 caracteres hexadecimales	Este valor se utiliza para instanciar el uso de la clave DUKPT inicial en el dispositivo receptor e identifica la clave inicial derivada de un BDK. Este campo normalmente contiene los datos de derivación pero no el contador. Utilice KS para TDES DUKPT.
KS	Número de serie de la clave inicial para el TDES DUKPT	20 caracteres hexadecimales	Este valor se utiliza para instanciar el uso de la clave DUKPT inicial en el dispositivo receptor e identifica la clave inicial derivada de un BDK. Este campo normalmente contiene los datos de derivación más un valor de contador puesto a cero. Utilice IK para AES DUKPT.

Nombre del encabezado	Finalidad	Validación típica	Notas
KP	KCV de la llave de embalaje	2 caracteres hexadecimales representan el método KCV (00 para el X9.24 método y 01 para el método CMAC). Seguido del valor KCV, que suele ser de 6 caracteres hexadecimales. Por ejemplo, 010FA329 representa el KCV de 0FA329 calculado mediante el método 01 (CMAC).	Este valor se utiliza para instanciar el uso de la clave DUKPT inicial en el dispositivo receptor e identifica la clave inicial derivada de un BDK. Este campo normalmen te contiene los datos de derivación más un valor de contador puesto a cero. Utilice IK para AES DUKPT.
PB	Bloque de relleno	caracteres ASCII imprimibles al azar	El servicio rellena automáticamente este campo al exportar para garantizar que los encabezados opcionales sean múltiplos de la longitud del bloque de cifrado

Exporte claves asimétricas (RSA)

Para exportar una clave pública en forma de certificado, utilice el get-public-key-certificate comando. Este comando devuelve:

- El certificado
- El certificado raíz

Ambos certificados están codificados en base64.

> **Note**
>
> Esta operación no es idempotente: las llamadas posteriores pueden generar certificados diferentes incluso si se utiliza la misma clave subyacente.

Example

```
$ aws payment-cryptography get-public-key-certificate \
     --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/5dza7xqd6soanjtb
```

```
{
"KeyCertificate": "LS0tLS1CRUdJTi...",
"KeyCertificateChain": "LS0tLS1CRUdJT..."
}
```

Temas avanzados

En esta sección se describen escenarios y configuraciones avanzados de intercambio de claves.

Temas

- Traiga su propia autoridad de certificación (BYOCA)
- Intercambio de claves físicas

Traiga su propia autoridad de certificación (BYOCA)

De forma predeterminada, cuando se necesita un certificado de clave pública para las claves asimétricas (RSA, ECC) creadas en el servicio, estos certificados los emite una autoridad de certificación (CA) de criptografía de AWS pagos y única para cada cuenta. Su objetivo es facilitar su uso X.509 sin la carga de identificar o configurar una CA o gestionar las solicitudes de firma de certificados (CSR).

AWS La criptografía de pagos también permite utilizar su propia CA cuando sea necesario por motivos normativos o de cumplimiento.

Descripción general de

La función BYOCA le permite utilizar su propia autoridad de certificación en cualquier lugar donde se utilicen certificados TR-34 import/export, incluidos RSA Unwrap y transferencias de claves. ECDH-based Esto resulta útil cuando necesita mantener una cadena de certificados coherente en toda la organización o cuando trabaja con socios que requieren certificados de CA específicos. El siguiente ejemplo muestra el flujo de trabajo de BYOCA mediante la exportación de TR-34 claves.

Las tres diferencias clave en comparación con el flujo de TR-34 exportación estándar son:

1. La clave RSA de firma se crea explícitamente mediante CreateKey. Anteriormente, se creaba implícitamente mediante. GetParametersForExport
2. Una nueva API GetCertificateSigningRequestcrea una solicitud de firma de certificado (CSR) que puede firmar una entidad emisora de certificados externa.
3. La ExportKeyAPI se ha ampliado para permitir que se proporcione un certificado en tiempo de ejecución. Anteriormente, esto lo proporcionaba implícitamente`import-token`, que pasa a ser un campo opcional.

⚠ Consideraciones importantes

- En estos ejemplos se utilizan RSA-2048 claves y se envuelve una TDES-2KEY clave. Al exportar AES-128, asegúrese de que todas las claves estén en RSA-3072 o RSA-4096.
- El error más común es que la clave representada por `SigningKeyIdentifier` y `SigningKeyCertificate` no coincide.

Flujo de trabajo BYOCA

Los siguientes pasos muestran el flujo de trabajo completo de BYOCA para la exportación. TR-34

Steps

- Paso 1: Crear una clave RSA
- Paso 2: generar una solicitud de firma de certificado
- Paso 3: Revise la CSR (opcional)
- Paso 4: firme la CSR con una autoridad de certificación
- Paso 5: Importar el certificado de CA

- Paso 6: Obtenga el certificado de cifrado KRD
- Paso 7: Exportar la clave con BYOCA

Paso 1: Crear una clave RSA

Primero, cree un par de claves RSA que, en última instancia, será el certificado de firma de KDH. Puede añadir etiquetas para identificar el propósito de la clave.

Example Cree una clave RSA para firmar

```
$ aws payment-cryptography create-key --exportable \
    --key-attributes
 KeyAlgorithm=RSA_2048,KeyUsage=TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE,KeyClass=ASYMMETRI
```

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-1:111122223333:key/
xgmq6fs6uow736uc",
        "KeyAttributes": {
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE",
            "KeyClass": "ASYMMETRIC_KEY_PAIR",
            "KeyAlgorithm": "RSA_2048",
            "KeyModesOfUse": {
                "Sign": true
            }
        },
        "KeyCheckValue": "41E3723C",
        "KeyCheckValueAlgorithm": "SHA_1",
        "Enabled": true,
        "Exportable": true,
        "KeyState": "CREATE_COMPLETE",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY"
    }
}
```

Tome nota de elloKeyArn, ya que lo necesitará en el siguiente paso.

Paso 2: generar una solicitud de firma de certificado

Genere una solicitud de firma de certificado (CSR) para que la firme su CA externa mediante la GetCertificateSigningRequestAPI. El resultado es un archivo PEM codificado en base64. Si decodifica el contenido en base64 y lo guarda, dispondrá de una CSR válida en formato PEM.

Example Genera CSR

```
$ aws payment-cryptography-data get-certificate-signing-request \
    --key-identifier arn:aws:payment-cryptography:us-east-1:111122223333:key/
xgmq6fs6uow736uc \
    --signing-algorithm SHA512 \
    --certificate-subject '{
        "CommonName": "MyCertificateAWSUSEAST",
        "Organization": "Amazon",
        "OrganizationUnit": "PaymentCryptography",
        "Country": "US",
        "StateOrProvince": "Virginia",
        "City": "Arlington"
    }'
```

```
{
    "CertificateSigningRequest": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0..."
}
```

El `CertificateSigningRequest` campo contiene la CSR codificada en base64 que enviará a su CA para que la firme.

Paso 3: Revise la CSR (opcional)

Si lo desea, puede utilizar OpenSSL para revisar el contenido de la CSR y asegurarse de que es válido y se ajusta a lo esperado.

Example Revise la CSR con OpenSSL

```
$ echo "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0..." | base64 -d | openssl req -
text
```

Paso 4: firme la CSR con una autoridad de certificación

Tras generar la CSR, es necesario que la firme una autoridad de certificación (CA). En los entornos de producción, normalmente Autoridad de certificación privada de AWS utilizaría la infraestructura

de CA establecida por su organización. Para realizar pruebas, puede usar OpenSSL para crear un certificado autofirmado.

Utilizando Autoridad de certificación privada de AWS

Para firmar la CSR con ella Autoridad de certificación privada de AWS, primero decodifique la CSR codificada en base64 y guárdela en un archivo y, a continuación, utilice la API. IssueCertificate

Example Firma la CSR con AWS Private CA

```
$ echo "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0..." | base64 -d > csr.pem

$ aws acm-pca issue-certificate \
    --certificate-authority-arn arn:aws:acm-pca:us-east-1:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012 \
    --csr fileb://csr.pem \
    --signing-algorithm SHA256WITHRSA \
    --validity Value=365,Type=DAYS
```

```
{
    "CertificateArn": "arn:aws:acm-pca:us-east-1:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/abcdef1234567890"
}
```

A continuación, recupere el certificado firmado:

Example Recupere el certificado firmado

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:us-east-1:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:us-east-1:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/abcdef1234567890
```

```
{
    "Certificate": "-----BEGIN CERTIFICATE-----\nMIID...\n-----END CERTIFICATE-----",
    "CertificateChain": "-----BEGIN CERTIFICATE-----\nMIID...\n-----END
 CERTIFICATE-----"
}
```

Guarde el contenido del certificado para usarlo en el paso de exportación. Deberás codificarlo en base64 cuando lo proporciones a la API. `ExportKey`

Uso de OpenSSL para realizar pruebas

Con fines de prueba, puede usar OpenSSL para crear una CA autofirmada y firmar la CSR. En primer lugar, cree una clave privada de CA y un certificado autofirmado:

Example Cree una CA de prueba con OpenSSL

```
$ # Generate CA private key
openssl genrsa -out ca-key.pem 4096

$ # Create self-signed CA certificate
openssl req -new -x509 -days 3650 -key ca-key.pem -out ca-cert.pem \
    -subj "/C=US/ST=Virginia/L=Arlington/O=TestOrg/CN=Test CA"
```

A continuación, decodifique la CSR del paso anterior y fírmela con su CA de prueba:

Example Firme CSR con OpenSSL

```
$ # Decode the base64-encoded CSR
echo "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0..." | base64 -d > csr.pem

$ # Sign the CSR with the CA
openssl x509 -req -in csr.pem -CA ca-cert.pem -CAkey ca-key.pem \
    -CAcreateserial -out signed-cert.pem -days 365 -sha512
```

```
Certificate request self-signature ok
subject=C=US, ST=Virginia, L=Arlington, O=Amazon, OU=PaymentCryptography,
 CN=MyCertificateAWSUSEAST
```

El certificado firmado ya está disponible. `signed-cert.pem` Deberás codificar este certificado en base64 cuando lo proporciones a la API: `ExportKey`

Example Codifique en Base64 el certificado firmado

```
$ cat signed-cert.pem | base64 -w 0
```

Paso 5: Importar el certificado de CA

En primer lugar, se debe confiar en cualquier CA que se utilice para evitar que se utilicen certificados arbitrarios. Importe el certificado raíz de su CA externa mediante la ImportKeyAPI. Si utiliza una CA intermedia, `import-key` vuelva a llamar, pero especifique `TrustedPublicKey` en lugar de `RootCertificatePublicKey` y especifique el ARN de la CA raíz.

Example Importe el certificado de CA raíz

```
$ aws payment-cryptography import-key --key-material='{
    "RootCertificatePublicKey": {
        "KeyAttributes": {
            "KeyAlgorithm": "RSA_4096",
            "KeyClass": "PUBLIC_KEY",
            "KeyModesOfUse": {
                "Verify": true
            },
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE"
        },
        "PublicKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0t..."
    }
}'
```

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-1:111122223333:key/
xivpaqy7qbbm7cdw",
        "KeyAttributes": {
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE",
            "KeyClass": "PUBLIC_KEY",
            "KeyAlgorithm": "RSA_4096",
            "KeyModesOfUse": {
                "Verify": true
            }
        },
        "Enabled": true,
        "KeyState": "CREATE_COMPLETE",
        "KeyOrigin": "EXTERNAL"
    }
}
```

Tome nota de las CA `KeyArn` para utilizarlas en el paso de exportación.

Paso 6: Obtenga el certificado de cifrado KRD

En este ejemplo, volvemos a importar a AWS Payment Cryptography, por lo que llamamos al servicio para recibir un certificado de clave pública KRD mediante la API. GetParametersForImport En un escenario real, lo proporcionaría otro sistema, como un HSM, un cajero automático, una terminal de pago o un sistema de gestión de terminales de pago.

Example Obtener parámetros para importación

```
$ aws payment-cryptography-data get-parameters-for-import \
    --key-material-type "TR34_KEY_BLOCK" \
    --wrapping-key-algorithm RSA_2048
```

```
{
    "WrappingKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0t...",
    "WrappingKeyCertificateChain": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0t...",
    "WrappingKeyAlgorithm": "RSA_2048",
    "ImportToken": "import-token-v2rxpl6drxeptn7w",
    "ParametersValidUntilTimestamp": "2025-11-01T18:45:31.271000-07:00"
}
```

Paso 7: Exportar la clave con BYOCA

Por último, exporte la clave TR-34 con su propio CA-signed certificado mediante la ExportKeyAPI. Proporcione el certificado de firma firmado por su CA externa.

Example TR-34 Exporte con BYOCA

```
$ aws payment-cryptography-data export-key \
    --export-key-identifier arn:aws:payment-cryptography:us-east-1:111122223333:key/
iox73p5f4c4yjiod \
    --key-material '{
        "Tr34KeyBlock": {
            "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-
cryptography:us-east-1:111122223333:key/j625deyfqlwctu57",
            "SigningKeyIdentifier": "arn:aws:payment-cryptography:us-
east-1:111122223333:key/xgmq6fs6uow736uc",
            "SigningKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0t...",
            "KeyBlockFormat": "X9_TR34_2012",
            "WrappingKeyCertificate": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0t..."
        }
```

```
    }'
```

```
{
    "WrappedKey": {
        "WrappedKeyMaterialFormat": "TR34_KEY_BLOCK",
        "KeyMaterial": "3082055A06092A864886F70D010702A082054B30820547...",
        "KeyCheckValue": "3DCA31",
        "KeyCheckValueAlgorithm": "ANSI_X9_24"
    }
}
```

El sistema receptor ahora puede importar el bloque de claves exportado mediante el proceso de TR-34 importación estándar.

Notas adicionales

- Estos ejemplos se muestran mediante la AWS CLI. La misma funcionalidad está disponible en todos los SDK de AWS, incluidos Java, Python, Go y Rust.
- Si realiza las pruebas con una CA autofirmada, puede usar OpenSSL para crear una CA de prueba y firmar la CSR. En producción, utilice la infraestructura de CA establecida de su organización.

Intercambio de claves físicas

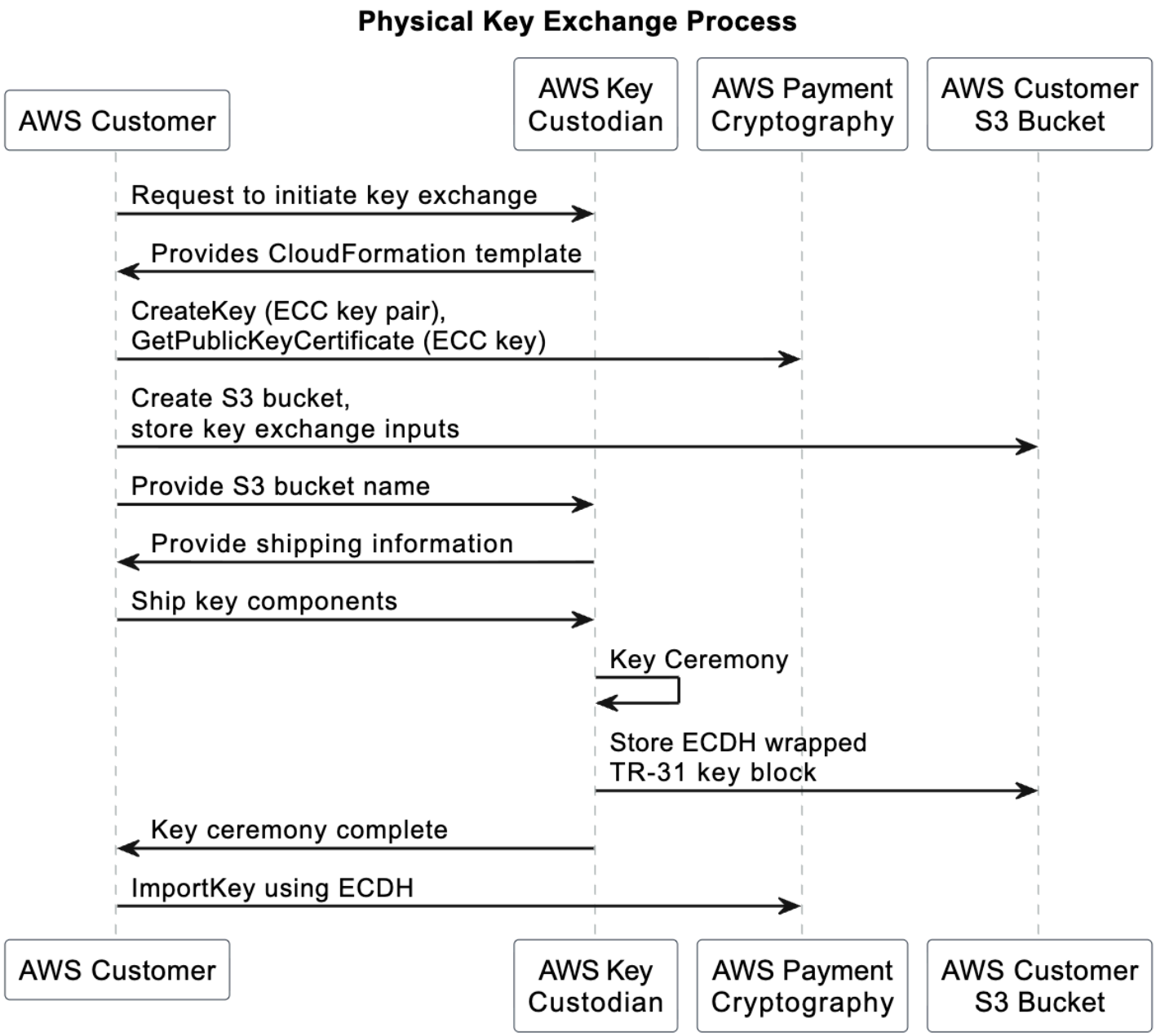
Puede utilizar Physical Key Exchange para convertir de forma segura los componentes de claves criptográficas en papel a formato electrónico cuando sus socios o proveedores no admitan el intercambio de claves electrónicas. Los custodios de AWS claves capacitados llevan a cabo las ceremonias clave en instalaciones AWS-operated seguras certificadas por PCI PIN y P2PE, y convierten los componentes clave en papel a formato electrónico mediante un HSM fuera de línea. El servicio utiliza el intercambio de ECDH-based claves para entregar un bloque de ECDH-wrapped TR-31 claves, que usted importa directamente a su cuenta de criptografía de pagos. AWS

> **Note**
>
> Recomendamos utilizar el sistema basado en estándares siempre Importación y exportación de claves que sea posible. Utilice Physical Key Exchange únicamente cuando sus socios o proveedores no admitan métodos electrónicos de intercambio de claves, como ANSI X9.24 TR-34, RSA wrap/unwrap o ECDH.

Cómo funciona el intercambio físico de claves

Para iniciar el intercambio de claves en papel, una CloudFormation plantilla le guiará a través de la configuración de los requisitos previos, incluida la creación de un par de claves ECC y un bucket S3 en su cuenta. Luego, usted o su socio envían los componentes clave en papel a la instalación AWS segura, donde los custodios de AWS llaves capacitados realizan la ceremonia de entrega de llaves mediante un HSM fuera de línea. El resultado es un bloque ECDH-wrapped TR-31 clave que se carga en el depósito de S3 y que se importa a la Importe las claves mediante técnicas asimétricas (ECDH) cuenta mediante este método. Physical Key Exchange permite importar claves KEK (uso de claves K1) o BDK (uso de claves B0) en los algoritmos de claves TDES y AES.

El siguiente diagrama muestra el proceso de intercambio de claves físicas de principio a fin.



1. Inicio: envía un ticket de soporte o trabaja con su administrador de cuentas para enviar una solicitud.
2. Configuración del cliente: la criptografía de AWS pagos proporciona una CloudFormation plantilla para que complete los siguientes pasos previos:
   - Cree un par de claves ECC P521 en su cuenta de criptografía AWS de pagos y recupere el certificado de clave pública.

- Cree un bucket de Amazon S3 con una política que conceda al servicio de criptografía de AWS pagos el read/write acceso principal.
- Guarde el certificado público de ECC y la CA raíz firmante en el bucket de Amazon S3.
- Proporcione los atributos clave: uso clave, modos de uso clave y número de componentes clave en papel que se enviarán.

3. Comparte el nombre del depósito de S3: el cliente comparte el nombre del depósito de S3 creado por la CloudFormation pila, donde se almacenan el certificado de clave pública, la cadena de certificados y los atributos clave para que AWS Payment Cryptography inicie el intercambio de claves.
4. Coordinación de envíos: la criptografía de AWS pagos proporciona los detalles de envío para una instalación US-based segura. Usted o su socio envían los componentes clave en papel a los custodios AWS clave.
5. Recibo de componentes: los custodios AWS clave reciben cada componente en papel y envían un acuse de recibo por separado para cada componente.
6. Ceremonia de clausura: los custodios de AWS llaves llevan a cabo la ceremonia de clausura utilizando un HSM desconectado. El bloque de TR-31 claves resultante, empaquetado con una ECDH-derived AES-256 clave, el certificado público ECC del HSM sin conexión y su certificado de firma se cargan en su bucket de Amazon S3.
7. Finalización: la criptografía AWS de pagos envía una confirmación de que se ha completado la ceremonia de entrega de llaves. A continuación, puede importar el bloque de TR-31 claves empaquetado en ECDH a su cuenta de criptografía de AWS pagos mediante este método. Importe las claves mediante técnicas asimétricas (ECDH)
8. Facturación: se le facturará por cada clave intercambiada al completar con éxito la ceremonia de entrega de llaves.

Seguridad y conformidad

Physical Key Exchange opera en instalaciones AWS seguras diseñadas para cumplir con los requisitos de seguridad física y lógica de PCI PIN y PCI P2PE. Se han establecido los siguientes controles:

Doble control y separación de funciones

AWS Los custodios clave se asignan a partir de diferentes equipos con estructuras de presentación de informes independientes. Existen procesos para garantizar que las principales etapas de las ceremonias se lleven a cabo bajo un doble control.

HSM fuera de línea

Las ceremonias clave se llevan a cabo utilizando módulos de seguridad de HSM-listed hardware PCI PTS certificados que funcionan sin conexión a la red. La clave nunca existe en texto sin cifrar fuera del límite del HSM.

Entrega de claves criptográficas

El material clave se transfiere desde el HSM desconectado a su cuenta de criptografía de AWS pagos mediante el intercambio de ECDH-based claves, lo que garantiza una protección criptográfica integral.

Auditoría y cumplimiento

AWS cuenta con procesos para cumplir con los requisitos de conformidad aplicables que se evalúan periódicamente para las certificaciones PCI, PIN y P2PE. Revise el paquete de cumplimiento de AWS Artifact para ver los informes a los que pueda hacer referencia en sus propias evaluaciones de PCI.

Uso de alias

Un alias es un nombre descriptivo para una clave de criptografía AWS de pagos. Por ejemplo, un alias le permite referirse a una clave como `alias/test-key` en lugar de `arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h`.

Puede usar un alias para identificar una clave en la mayoría de las operaciones de administración de claves (plano de control) y en las operaciones criptográficas (plano de datos).

También puedes permitir y denegar el acceso a la clave de criptografía de AWS pagos en función de sus alias sin editar las políticas ni gestionar las subvenciones. Esta característica forma parte de la compatibilidad del servicio con el control de acceso basado en atributos (ABAC).

Gran parte de la potencia de los alias proviene de su capacidad de cambiar la clave asociada a un alias en cualquier momento. Los alias pueden hacer que su código sea más fácil de escribir y mantener. Por ejemplo, supongamos que utiliza un alias para hacer referencia a una clave de criptografía de AWS pago concreta y desea cambiarla AWS . En ese caso, simplemente asocie el alias con una clave diferente. No necesita cambiar el código ni la configuración de su aplicación.

Los alias también facilitan la reutilización del mismo código en diferentes Regiones de AWS. Cree alias con el mismo nombre en varias regiones y asocie cada alias a una clave de criptografía de

AWS pagos en su región. Cuando el código se ejecuta en cada región, el alias hace referencia a la clave de criptografía de AWS pagos asociada en esa región.

Puedes crear un alias para una clave de criptografía de AWS pagos mediante la `CreateAlias` API.

La API AWS de criptografía de pagos proporciona un control total de los alias de cada cuenta y región. La API incluye operaciones para crear un alias (CreateAlias), ver los nombres de los alias y el keyARN vinculado (alias de lista), cambiar la clave de criptografía de AWS pagos asociada a un alias (update-alias) y eliminar un alias (delete-alias).

Temas

- Acerca de los alias
- Usar alias en las aplicaciones
- API relacionadas

Acerca de los alias

AWS Descubre cómo funcionan los alias en la criptografía de pagos.

Un alias es un recurso independiente AWS

> Un alias no es propiedad de una clave de criptografía de AWS pagos. Las acciones que realice en el alias no afectan a su clave asociada. Puede crear un alias para una clave de criptografía de AWS pago y, a continuación, actualizar el alias para que se asocie a una clave de criptografía de AWS pago diferente. Incluso puedes eliminar el alias sin que ello afecte a la clave de criptografía de AWS pagos asociada. Si elimina una clave de AWS Payment Cryptography, todos los alias asociados a esa clave quedarán sin asignar.
>
> Si especificas un alias como recurso en una política de IAM, la política se refiere al alias y no a la clave de criptografía de AWS pagos asociada.

Cada alias tiene un nombre coloquial

> Cuando cree un alias, especifique el nombre del alias precedido por `alias/`. Por ejemplo, `alias/test_1234`

Cada alias está asociado a una clave de criptografía AWS de pagos a la vez

> El alias y su clave AWS de criptografía de pagos deben estar en la misma cuenta y región.

Una clave de criptografía de AWS pago se puede asociar a más de un alias al mismo tiempo, pero cada alias solo se puede asignar a una clave

Por ejemplo, esta salida `list-aliases` muestra que el alias `alias/sampleAlias1` está asociado con exactamente una clave de AWS Payment Cryptography de destino, que está representada por la propiedad de `KeyArn`.

```
$ aws payment-cryptography list-aliases
```

```
  {
    "Aliases": [
        {
            "AliasName": "alias/sampleAlias1",
            "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h"
        }
    ]
}
```

Se pueden asociar varios alias a la misma clave de criptografía de pagos AWS

Por ejemplo, puede asociar los alias `alias/sampleAlias1;` y `alias/sampleAlias2` con la misma clave.

```
$ aws payment-cryptography list-aliases
```

```
{
        "Aliases": [
            {
                "AliasName": "alias/sampleAlias1",
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h"
            },
            {
                "AliasName": "alias/sampleAlias2",
```

```
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h"
            }
        ]
    }
```

El alias debe ser único para una cuenta y región determinadas.

Por ejemplo, solo puede tener un alias `alias/sampleAlias1` en cada cuenta y región. Los alias distinguen entre mayúsculas y minúsculas, pero le recomendamos que no utilice alias que sólo difieran en las mayúsculas, ya que pueden dar lugar a errores. No puede cambiar un nombre de alias. Sin embargo, puede eliminar el alias y crear un nuevo alias con el nombre deseado.

Puede crear alias con el mismo nombre en diferentes regiones

Por ejemplo, puede tener un alias `alias/sampleAlias2` en el Este de EE. UU. (Norte de Virginia) y un alias `alias/sampleAlias2` en el Oeste de EE. UU. (Oregón). Cada alias estaría asociado a una clave de criptografía AWS de pagos en su región. Si su código se refiere a un nombre de alias como `alias/finance-key`, puede ejecutarlo en varias regiones. En cada región, utiliza una diferente alias/sampleAlias2. Para obtener más información, consulte Usar alias en las aplicaciones.

Puede cambiar la clave de criptografía de AWS pago asociada a un alias

Puede utilizar la `UpdateAlias` operación para asociar un alias a una clave de criptografía AWS de pagos diferente. Por ejemplo, si el `alias/sampleAlias2` alias está asociado a la clave de criptografía de `arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h` AWS pagos, puede actualizarlo para que esté asociado a la `arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi` clave.

> **Warning**
>
> AWS La criptografía de pagos no valida que la clave antigua y la nueva tengan los mismos atributos, como el uso de claves. La actualización con un tipo de clave diferente puede dar lugar a problemas en su aplicación.

Algunas claves no tienen alias

Un alias es una característica opcional y no todas las claves tendrán alias a menos que elija operar su entorno de esta manera. Las claves pueden asociarse con alias utilizando el comando `create-alias`. Además, puede usar la operación update-alias para cambiar la clave de AWS Payment Cryptography asociada a un alias y la operación delete-alias para eliminar un alias. Como resultado, es posible que algunas claves de criptografía de AWS pagos tengan varios alias y que otras no tengan ninguno.

Asignación de una clave a un alias

Puede asignar una clave (representada por un ARN) a uno o más alias utilizando el comando `create-alias`. Este comando no es idempotente; para actualizar un alias, utilice el comando update-alias.

```
$ aws payment-cryptography create-alias --alias-name alias/sampleAlias1 \
             --key-arn arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h
```

```
{
    "Alias": {
        "AliasName": "alias/alias/sampleAlias1",
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h"
    }
}
```

Usar alias en las aplicaciones

Puedes usar un alias para representar una clave de criptografía AWS de pagos en el código de tu aplicación. El `key-identifier` parámetro en las operaciones de datos de criptografía de AWS pagos, así como en otras operaciones como List Keys, acepta un alias o un alias ARN.

```
$ aws payment-cryptography-data generate-card-validation-data --key-identifier alias/
BIN_123456_CVK --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue2={CardExpiryDate=0123}
```

Cuando utilice un ARN de alias, recuerde que la asignación de alias a una clave de criptografía de AWS pago se define en la cuenta propietaria de la clave de criptografía de AWS pago y puede diferir en cada región.

Uno de los usos más potentes de los alias es en aplicaciones que se ejecutan en múltiples Regiones de AWS.

Puede crear una versión diferente de la aplicación en cada región o utilizar un diccionario, una configuración o una sentencia de cambio para seleccionar la clave criptográfica de AWS pagos adecuada para cada región. Pero puede ser más fácil crear un alias con el mismo nombre de alias en cada región. El nombre del alias distingue entre mayúsculas y minúsculas.

API relacionadas

Etiquetas

Las etiquetas son pares de claves y valores que actúan como metadatos para organizar las claves de criptografía AWS de pagos. Pueden utilizarse para identificar claves de forma flexible o agrupar una o varias claves.

Obtener claves

Una clave AWS de criptografía de pago representa una sola unidad de material criptográfico y solo se puede utilizar para las operaciones criptográficas de este servicio. La GetKeys API toma KeyIdentifier como entrada y devuelve los metadatos clave, incluidos los atributos, el estado y las marcas de tiempo, pero no devuelve el material clave criptográfico real.

Example

```
$ aws payment-cryptography get-key --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h
```


```
{
  "Key": {
      "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
      "KeyAttributes": {
          "KeyUsage": "TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY",
          "KeyClass": "SYMMETRIC_KEY",
          "KeyAlgorithm": "AES_128",
          "KeyModesOfUse": {
              "Encrypt": true,
              "Decrypt": true,
              "Wrap": true,
              "Unwrap": true,
              "Generate": false,
              "Sign": false,
              "Verify": false,
              "DeriveKey": false,
              "NoRestrictions": false
          }
      },
      "KeyCheckValue": "0A3674",
      "KeyCheckValueAlgorithm": "CMAC",
      "Enabled": true,
      "Exportable": true,
      "KeyState": "CREATE_COMPLETE",
      "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
      "CreateTimestamp": "2023-06-02T07:38:14.913000-07:00",
      "UsageStartTimestamp": "2023-06-02T07:38:14.857000-07:00"
  }
}
```

Haga que el público key/certificate se asocie a un key pair

Get Public Key/Certificate devuelve la clave pública indicada por`KeyArn`. Puede ser la parte de clave pública de un par de claves generado en la criptografía de AWS pago o una clave pública importada anteriormente. El caso de uso más común es proporcionar la clave pública a un servicio externo que cifrará datos. Luego, esos datos se pueden pasar a una aplicación que utilice la criptografía de AWS pago y se pueden descifrar con la clave privada protegida en la criptografía de pago. AWS

El servicio devuelve las claves públicas como un certificado público. El resultado de la API contiene la CA y el certificado de clave pública. Ambos elementos de datos están codificados en base64.

> **Note**
>
> El certificado público devuelto está pensado para ser de corta duración y no pretende ser idempotente. Es posible que reciba un certificado diferente en cada llamada a la API, aunque la clave pública en sí no cambie.

Example

```
$ aws payment-cryptography get-public-key-certificate  --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/nsq2i3mbg6sn775f
```

```
{
  "KeyCertificate":
 "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUV2VENDQXFXZ0F3SUJBZ0lSQUo1OWd2VkpDd3dlYldMNldYZEpYY
  "KeyCertificateChain":
 "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUY0VENDQThtZ0F3SUJBZ0lSQUtlN2piaHFKZjJPd3FGUWI5c3VuC
}
```

Etiquetado de claves

En la criptografía de AWS pagos, puede añadir etiquetas a una clave de criptografía de AWS pagos al crear una clave, y etiquetar o desetiquetar las claves existentes, a menos que estén pendientes de ser eliminadas. Las etiquetas son opcionales, pero pueden ser muy útiles.

Para obtener información general sobre las etiquetas, incluidas las prácticas recomendadas, las estrategias de etiquetado y el formato y la sintaxis de las etiquetas, consulte los recursos de etiquetado AWS en. Referencia general de Amazon Web Services

Temas

- Acerca de las etiquetas en la criptografía de pagos AWS
- Visualización de etiquetas clave en la consola
- Administración de etiquetas de clave con operaciones de la API
- Control del acceso a las etiquetas
- Uso de etiquetas para controlar el acceso a las claves

Acerca de las etiquetas en la criptografía de pagos AWS

Una etiqueta es una etiqueta de metadatos opcional que puede asignar (o AWS puede asignar) a un AWS recurso. Cada etiqueta consta de una clave de etiqueta y a valor de etiqueta, que distinguen entre mayúsculas y minúsculas. El valor de la etiqueta puede ser una cadena vacía (nula). Cada etiqueta de un recurso debe tener una clave de etiqueta diferente, pero puedes añadir la misma etiqueta a varios AWS recursos. Cada recurso puede tener un máximo de 50 etiquetas creadas por el usuario.

No incluya información confidencial en la clave ni en el valor de la etiqueta. Muchas personas pueden acceder a las etiquetas Servicios de AWS, incluida la facturación.

En la criptografía de AWS pagos, puede añadir etiquetas a una clave al crearla y etiquetar o desetiquetar las claves existentes, a menos que estén pendientes de ser eliminadas. No puede etiquetar alias. Las etiquetas son opcionales, pero pueden ser muy útiles.

Por ejemplo, puede añadir una `"Project"="Alpha"` etiqueta a todas las claves de criptografía de AWS pagos y a los buckets de Amazon S3 que utilice para el proyecto Alpha. Otro ejemplo es añadir una etiqueta `"BIN"="20130622"` a todas las claves asociadas a un número de identificación bancaria (BIN) específico.

```
    [
    {
      "Key": "Project",
      "Value": "Alpha"
    },
    {
      "Key": "BIN",
      "Value": "20130622"
    }
  ]
```

Para obtener información general sobre las etiquetas, incluidos el formato y la sintaxis, consulte AWS los recursos de etiquetado en. Referencia general de Amazon Web Services

Las etiquetas lo ayudan a hacer lo siguiente:

- Identifique y organice sus AWS recursos. Muchos AWS servicios admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, puede asignar la misma etiqueta a una clave de criptografía de AWS pagos y a un volumen o secreto de Amazon Elastic Block Store (Amazon EBS). AWS Secrets Manager También puede utilizar etiquetas para identificar claves para la automatización.
- Realice un seguimiento de sus costes. AWS Cuando agrega etiquetas a sus AWS recursos, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Puede usar esta función para realizar un seguimiento de los costos de criptografía de AWS pagos de un proyecto, aplicación o centro de costos.

  Para obtener más información sobre el uso de etiquetas para la asignación de costos, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing . Para obtener información sobre las reglas de las claves y los valores de las etiquetas, consulte las restricciones de User-Defined etiquetas en la Guía del AWS Billing usuario.
- Controle el acceso a sus AWS recursos. Permitir y denegar el acceso a las claves en función de sus etiquetas forma parte del apoyo de la criptografía de AWS pagos al control de acceso basado en atributos (ABAC). Para obtener más información sobre el control de acceso a AWS Payment Cryptography basado en etiquetas, consulte Autorización basada en etiquetas de criptografía de pago AWS. Para obtener más información general sobre el uso de etiquetas para controlar el

acceso a AWS los recursos, consulte Control del acceso a los AWS recursos mediante etiquetas de recursos en la Guía del usuario de IAM.

AWS La criptografía de pagos escribe una entrada en su AWS CloudTrail registro cuando utiliza las operaciones TagResource UntagResource, o ListTagsForResource .

Visualización de etiquetas clave en la consola

Para ver las etiquetas en la consola, necesita permiso de etiquetado en la clave desde una política de IAM que incluya la clave. Necesita estos permisos además de los permisos para ver las claves en la consola.

Administración de etiquetas de clave con operaciones de la API

Puede utilizar la API de AWS Payment Cryptography para agregar, eliminar y enumerar etiquetas para las claves que administre. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido. No puedes etiquetar Claves administradas por AWS.

Para agregar, editar, ver y eliminar etiquetas de una clave, debe tener los permisos necesarios. Para obtener más información, consulte Control del acceso a las etiquetas.

Temas

- CreateKey: Añadir etiquetas a una clave nueva
- TagResource: Añada o cambie las etiquetas de una clave
- ListResourceTags: Obtenga las etiquetas de una clave
- UntagResource: elimina las etiquetas de una clave

CreateKey: Añadir etiquetas a una clave nueva

Puede añadir etiquetas cuando cree una llave. Para especificar las etiquetas, utilice el `Tags` parámetro de la CreateKeyoperación.

Para agregar etiquetas al crear una clave, la persona que llama debe tener el permiso `payment-cryptography:TagResource` en una política de IAM. Como mínimo, el permiso debe cubrir todas las claves de la cuenta y la región. Para obtener más información, consulte Control del acceso a las etiquetas.

El valor del parámetro `Tags` de `CreateKey` es una colección de pares de claves y valores de etiqueta que distinguen mayúsculas y minúsculas. Cada etiqueta de una clave debe tener un nombre de etiqueta diferente. El valor de etiqueta puede ser una cadena vacía o nula.

Por ejemplo, el siguiente AWS CLI comando crea una clave de cifrado simétrica con una `Project:Alpha` etiqueta. Cuando especifique más de un par de clave-valor, utilice un espacio para separar cada par.

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY, \
       KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY, \
       KeyModesOfUse='{Generate=true,Verify=true}' \
       --tags '[{"Key":"Project","Value":"Alpha"},{"Key":"BIN","Value":"123456"}]'
```

Cuando este comando se ejecuta correctamente, devuelve un objeto `Key` con información sobre la nueva clave. Sin embargo, `Key` no incluye etiquetas. Para obtener las etiquetas, utilice la ListResourceTagsoperación.

TagResource: Añada o cambie las etiquetas de una clave

La TagResourceoperación añade una o más etiquetas a una clave. No puede usar esta operación para agregar o editar etiquetas en una Cuenta de AWS diferente.

Para agregar una etiqueta, especifique una clave de etiqueta nueva y un valor de la etiqueta. Para editar una etiqueta, especifique una clave de etiqueta existente y un nuevo valor de etiqueta. Cada etiqueta de una clave debe tener una clave de etiqueta distinta. El valor de etiqueta puede ser una cadena vacía o nula.

Por ejemplo, el siguiente comando agrega las etiquetas **`UseCase`** y **`BIN`** a una clave de ejemplo.

```
$ aws payment-cryptography tag-resource --resource-arn arn:aws:payment-
cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h --tags
 '[{"Key":"UseCase","Value":"Acquiring"},{"Key":"BIN","Value":"123456"}]'
```

Si este comando se realiza correctamente, no devuelve ningún resultado. Para ver las etiquetas de una tecla, utilice la ListResourceTagsoperación.

También pueden utilizar TagResource para cambiar los valores de una etiqueta existente. Para sustituir los valores de etiqueta, especifique la misma clave de etiqueta con distintos valores. Las etiquetas no listadas en un comando de modificación no se cambian ni se eliminan.

Por ejemplo, este comando cambia el valor de la etiqueta `Project` de `Alpha` a `Noe`.

El comando volverá http/200 sin contenido. Para ver los cambios, utilice `ListTagsForResource`

```
$ aws payment-cryptography tag-resource --resource-arn arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h \
        --tags '[{"Key":"Project","Value":"Noe"}]'
```

ListResourceTags: Obtenga las etiquetas de una clave

La ListResourceTagsoperación obtiene las etiquetas de una clave. El parámetro `ResourceArn` (keyArn o keyAlias) es obligatorio. No puede usar esta operación para ver las etiquetas de claves en una Cuenta de AWS diferente.

Por ejemplo, el comando siguiente obtiene las etiquetas para una clave de ejemplo.

```
$ aws payment-cryptography list-tags-for-resource --resource-arn arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h

  {
    "Tags": [
        {
            "Key": "BIN",
            "Value": "20151120"
        },
        {
            "Key": "Project",
            "Value": "Production"
        }
    ]
}
```

UntagResource: elimina las etiquetas de una clave

La UntagResourceoperación elimina las etiquetas de una clave. Para identificar las etiquetas que desea eliminar, especifique las claves de etiqueta. No puede usar esta operación para eliminar etiquetas de claves una Cuenta de AWS diferente.

Cuando tiene éxito, la operación `UntagResource` no devuelve ningún resultado. Además, si la clave de etiqueta especificada no se encuentra en la clave, no arroja una excepción ni devuelve una respuesta. Para confirmar que la operación ha funcionado, utilice la ListResourceTagsoperación.

Por ejemplo, este comando elimina la etiqueta **`Purpose`** y todos sus valores de la clave especificada.

```
$ aws payment-cryptography untag-resource \
       --resource-arn arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h --tag-keys Project
```

Control del acceso a las etiquetas

Para agregar, ver y eliminar etiquetas mediante el uso de la API, las entidades principales necesitan permisos de etiquetado en la política de IAM.

También puede limitar estos permisos mediante el uso de claves de condición AWS globales para las etiquetas. En la criptografía de AWS pagos, estas condiciones pueden controlar el acceso a las operaciones de etiquetado, como TagResourcey. UntagResource

Para obtener más información y políticas de ejemplo, consulte Control del acceso en función de las claves de etiquetaen la Guía del usuario de IAM.

Los permisos para crear y administrar etiquetas funcionan de la siguiente manera.

criptografía de pagos: TagResource

Permite a las entidades principales agregar o editar etiquetas. Para agregar etiquetas al crear una clave, la entidad principal debe tener permiso en una política de IAM que no esté restringida a determinadas claves.

criptografía de pago: ListTagsForResource

Permite a las entidades principales ver etiquetas en claves.

criptografía de pago: UntagResource

Permite a las entidades principales eliminar etiquetas de las claves.

Permisos de etiquetas en políticas

Puede proporcionar permisos de etiquetas en una política de claves o una política de IAM. Por ejemplo, la siguiente política de claves de ejemplo ofrece permiso de etiquetar a los usuarios seleccionados en la clave. Da permiso a todos los usuarios que pueden asumir los roles de administrador o desarrollador de ejemplo para ver etiquetas.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "example-key-policy",
  "Statement": [
    {
      "Sid": "EnableIAMUserPermissions",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
      "Action": "payment-cryptography:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowAllTaggingPermissions",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/LeadAdmin",
        "arn:aws:iam::111122223333:user/SupportLead"
      ]},
      "Action": [
        "payment-cryptography:TagResource",
        "payment-cryptography:ListTagsForResource",
        "payment-cryptography:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow roles to view tags",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/Administrator",
          "arn:aws:iam::111122223333:role/Developer"
        ]
      },
      "Action": "payment-cryptography:ListTagsForResource",
      "Resource": "*"
    }
  ]
}
```

Para conceder permiso de etiquetado de entidades principales en varias claves, puede usar una política de IAM. Para que esta política sea efectiva, la política de claves de cada clave debe permitir a la cuenta utilizar políticas de IAM para controlar el acceso a clave.

Por ejemplo, la siguiente política de IAM permite a las entidades principales crear claves. También les permite crear y administrar etiquetas en todas las claves de la cuenta especificada. Esta combinación permite a los directores utilizar el parámetro tags de la CreateKeyoperación para añadir etiquetas a una clave mientras la crean.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKeys",
      "Effect": "Allow",
      "Action": "payment-cryptography:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyTags",
      "Effect": "Allow",
      "Action": [
        "payment-cryptography:TagResource",
        "payment-cryptography:UntagResource",
        "payment-cryptography:ListTagsForResource"
      ],
      "Resource": "arn:aws:payment-cryptography:*:111122223333:key/*"
    }
  ]
}
```

Limitar los permisos de etiqueta

Puede limitar los permisos de etiquetado mediante condiciones de política. Las siguientes condiciones de política se pueden aplicar a los permisos `payment-cryptography:TagResource` y `payment-cryptography:UntagResource`. Por ejemplo, puede utilizar la condición `aws:RequestTag/`*`tag-key`* para permitir que una entidad principal agregue solo etiquetas particulares, o impedir que una entidad principal agregue etiquetas con claves de etiqueta concretas.

- fuiste: RequestTag
- aws:ResourceTag/tag-key (solo políticas de IAM)
- AWS: TagKeys

Como práctica recomendada cuando utilice etiquetas para controlar el acceso a claves, utilice la clave de condición `aws:RequestTag/tag-key` o `aws:TagKeys` para determinar qué etiquetas (o claves de etiqueta) están permitidas.

Por ejemplo, la siguiente política IAM es similar a la anterior. Sin embargo, esta política permite a las entidades principales crear etiquetas (`TagResource`) y eliminar etiquetas `UntagResource` solo para etiquetas con una clave de etiqueta `Project`.

Como `TagResource` las `UntagResource` solicitudes pueden incluir varias etiquetas, debe especificar un operador `ForAllValues` o `ForAnyValue` configurarlo con la TagKeys condición aws:. El operador `ForAnyValue` requiere que al menos una de las claves de etiqueta de la solicitud coincida con una de las claves de etiqueta de la política. El operador `ForAllValues` requiere que todas las claves de etiqueta de la solicitud coincidan con una de las claves de etiqueta de la política. El `ForAllValues` operador también devuelve el `true` mensaje si no hay etiquetas en la solicitud, pero TagResource no lo UntagResource hace si no se especifica ninguna etiqueta. Para obtener información detallada sobre los operadores de conjunto, consulte Usar varias claves y valores en la Guía del usuario de IAM.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKey",
      "Effect": "Allow",
      "Action": "payment-cryptography:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyViewAllTags",
      "Effect": "Allow",
      "Action": "payment-cryptography:ListTagsForResource",
      "Resource": "arn:aws:payment-cryptography:*:111122223333:key/*"
    },
```

```
    {
      "Sid": "IAMPolicyManageTags",
      "Effect": "Allow",
      "Action": [
        "payment-cryptography:TagResource",
        "payment-cryptography:UntagResource"
      ],
      "Resource": "arn:aws:payment-cryptography:*:111122223333:key/*",
      "Condition": {
          "ForAllValues:StringEquals": {"aws:TagKeys": "Project"}
      }
    }
  ]
}
```

Uso de etiquetas para controlar el acceso a las claves

Puede controlar el acceso a la criptografía de AWS pagos en función de las etiquetas de la clave. Por ejemplo, puede escribir una política de IAM que permita a las entidades principales habilitar y desactivar solo las claves que tienen una etiqueta concreta. O bien, puede utilizar una política de IAM para evitar que las entidades principales utilicen claves en operaciones criptográficas, a menos que la clave tenga una etiqueta concreta.

Esta función forma parte del soporte de criptografía de AWS pagos para el control de acceso basado en atributos (ABAC). Para obtener información sobre el uso de etiquetas para controlar el acceso a AWS los recursos, consulta ¿Para qué sirve el ABAC? AWS y Cómo controlar el acceso a AWS los recursos mediante etiquetas de recursos en la Guía del usuario de IAM.

AWS La criptografía de pagos admite la clave contextual de condición global aws:ResourceTag/tag-key, que permite controlar el acceso a las claves en función de las etiquetas de la clave. Dado que varias claves pueden tener la misma etiqueta, esta función le permite aplicar el permiso a un conjunto seleccionado de claves. También puede cambiar fácilmente las claves del conjunto cambiando sus etiquetas.

En la criptografía AWS de pagos, la clave de `aws:ResourceTag/tag-key` condición solo se admite en las políticas de IAM. No se admite en las políticas clave, que se aplican solo a una clave, ni en las operaciones que no utilizan una clave en particular, como las operaciones ListKeyso ListAliases.

Controlar el acceso con etiquetas proporciona una forma sencilla, escalable y flexible de administrar los permisos. Sin embargo, si no está diseñado y administrado correctamente, puede permitir o denegar el acceso a sus claves inadvertidamente. Si utiliza etiquetas para controlar el acceso, tenga en cuenta las siguientes prácticas.

- Utilice etiquetas para reforzar la práctica recomendada de acceso menos privilegiado. Proporcione a las entidades principales de IAM solo los permisos que necesitan y únicamente en las claves de que deben usar o administrar. Por ejemplo, utilice etiquetas para etiquetar las claves utilizadas en un proyecto. A continuación, dé permiso al equipo del proyecto para usar solo claves con la etiqueta de proyecto.
- Tenga cuidado al dar a las entidades principales los permisos `payment-cryptography:TagResource` y `payment-cryptography:UntagResource` que les permiten agregar, editar y eliminar etiquetas. Cuando utiliza etiquetas para controlar el acceso a las claves, cambiar una etiqueta puede dar permiso a las entidades principales para usar claves que de otro modo no tenían permiso para usar. También puede denegar el acceso a las claves que otras entidades principales requieren para realizar sus trabajos. Los administradores de claves que no tienen permiso para cambiar políticas de claves o crear concesiones pueden controlar el acceso a claves si tienen permiso para administrar etiquetas.

  Siempre que sea posible, utilice una condición de política, como `aws:RequestTag/`*`tag-key`* o `aws:TagKeys` para limitar los permisos de etiquetado de una entidad principal a determinadas etiquetas o patrones de etiquetas en determinadas claves.
- Revisa los elementos principales Cuenta de AWS que actualmente tienen permisos para etiquetar y desetiquetar y ajústalos si es necesario. Las políticas de IAM pueden habilitar permisos de etiqueta y desetiqueta en todas las claves. Por ejemplo, la política Admin permite a las entidades principales administradas etiquetar, desetiquetar y generar un lista de etiquetas en todas las claves.
- Antes de establecer una política que dependa de una etiqueta, revisa las etiquetas de las claves de tu. Cuenta de AWS Asegúrese de que su política solo se aplique a las etiquetas que desea incluir. Usa CloudTrail registros y CloudWatch alarmas para avisarte de los cambios en las etiquetas que puedan afectar al acceso a tus llaves.
- Las condiciones de política basadas en etiquetas utilizan la coincidencia de patrones; no están vinculadas a una instancia concreta de una etiqueta. Una política que utiliza claves de condición basadas en etiquetas afecta a todas las etiquetas nuevas y existentes que coincidan con el patrón. Si elimina y vuelve a crear una etiqueta que coincida con una condición de política, la condición se aplica a la nueva etiqueta, igual que a la anterior.

Por ejemplo, tomemos el siguiente ejemplo de política de IAM. Permite a las entidades principales llamar a las operaciones de Descifrado sólo en claves de su cuenta que sean de la región Este de EE. UU. (Norte de Virginia) y tengan una etiqueta `"Project"="Alpha"`. Puede adjuntar esta política a roles del ejemplo de proyecto Alpha.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "payment-cryptography:DecryptData"
      ],
      "Resource": "arn:aws:payment-cryptography:us-east-1:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

La siguiente política de IAM de ejemplo permite a la entidad principal utilizar la clave en la cuenta para operaciones criptográficas. Pero prohíbe a las entidades principales usar estas operaciones criptográficas en claves con una etiqueta `"Type"="Reserved"` o sin etiqueta `"Type"`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "IAMAllowCryptographicOperations",
      "Effect": "Allow",
      "Action": [
        "payment-cryptography:EncryptData",
```

```
        "payment-cryptography:DecryptData",
        "payment-cryptography:ReEncrypt*"
      ],
      "Resource": "arn:aws:payment-cryptography:*:111122223333:key/*"
    },
    {
      "Sid": "IAMDenyOnTag",
      "Effect": "Deny",
      "Action": [
        "payment-cryptography:EncryptData",
        "payment-cryptography:DecryptData",
        "payment-cryptography:ReEncrypt*"
      ],
      "Resource": "arn:aws:payment-cryptography:*:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Type": "Reserved"
        }
      }
    },
    {
      "Sid": "IAMDenyNoTag",
      "Effect": "Deny",
      "Action": [
       "payment-cryptography:EncryptData",
       "payment-cryptography:DecryptData",
       "payment-cryptography:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/Type": "true"
        }
      }
    }
  ]
}
```

Comprender los atributos clave de la clave AWS de criptografía de pagos

Un principio de la gestión adecuada de claves es que éstas tengan un alcance apropiado y sólo puedan utilizarse para operaciones permitidas. Como tal, ciertas claves sólo pueden crearse con ciertos modos de uso. Siempre que sea posible, esto se alinea con los modos de uso disponibles, tal como se definen en. TR-31

Si bien la criptografía de AWS pagos le impedirá crear claves no válidas, aquí encontrará combinaciones válidas para su comodidad.

Claves simétricas

- TR31_B0_BASE_DERIVATION_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación permitida de modos de uso clave: { DeriveKey = true}, { NoRestrictions = true}
- TR31_C0_CARD_VERIFICATION_KEY
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions
- TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación de modos de uso clave permitida: {Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true}, {Encrypt = true}, {Decrypt = true, Unwrap = true}, {= true} NoRestrictions
- TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY*, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {= true} DeriveKey , {= true} NoRestrictions
- TR31_E1_EMV_MKEY_CONFIDENTIALITY
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {= true DeriveKey }, {= true} NoRestrictions
- TR31_E2_EMV_MKEY_INTEGRITY
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {= true DeriveKey }, {= true} NoRestrictions

- TR31_E4_EMV_MKEY_DYNAMIC_NUMBERS
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {= true DeriveKey }, {= true} NoRestrictions
- TR31_E5_EMV_MKEY_CARD_PERSONALIZATION
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {= true DeriveKey }, {= true} NoRestrictions
- TR31_E6_EMV_MKEY_OTHER
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY, AES_128*, AES_192*, AES_256*
  - Combinación permitida de modos de uso clave: {= true DeriveKey }, {= true} NoRestrictions
- TR31_K0_KEY_ENCRYPTION_KEY
  - Se recomienda utilizar TR31_K1_KEY_BLOCK_PROTECTION_KEY. Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación permitida de modos de uso clave: {Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true}, {Encrypt = true, Wrap = true}, {= true} NoRestrictions
- TR31_K1_KEY_BLOCK_PROTECTION_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación permitida de modos de uso clave: {Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true}, {Encrypt = true, Wrap = true}, {Decrypt = true, Unwrap = true}, { NoRestrictions = true}
- TR31_M1_ISO_9797_1_MAC_KEY
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY
  - Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions
- TR31_M3_ISO_9797_3_MAC_KEY
  - Algoritmos clave permitidos: TDES_2KEY, TDES_3KEY
  - Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions
- TR31_M6_ISO_9797_5_CMAC_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions
- TR31_M7_HMAC_KEY

- Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
- Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions

- TR31_P0_PIN_ENCRYPTION_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación de modos de uso clave permitida: {Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true}, {Encrypt = true}, {Decrypt = true, Unwrap = true}, {= true} NoRestrictions
- TR31_V1_IBM3624_PIN_VERIFICATION_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions
- TR31_V2_VISA_PIN_VERIFICATION_KEY
  - Algoritmos de clave permitidos: TDES_2KEY, TDES_3KEY, AES_128, AES_192, AES_256
  - Combinación permitida de modos de uso clave: {Generate = true}, {Verify = true}, {Generate = true, Verify= true}, {= true} NoRestrictions

Claves asimétricas

- TR31_D1_ASYMMETRIC_KEY_FOR_DATA_ENCRYPTION
  - Algoritmos de clave permitidos: RSA_2048, RSA_3072, RSA_4096
  - Combinación permitida de modos de uso clave: {Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true}, {Encrypt = true, Wrap = true}, {Decrypt = true, Unwrap = true}, {NoRestrictions = true}
  - NOTA: {Encrypt = true, Wrap = true} es la única opción válida al importar una clave pública destinada a cifrar datos o empaquetar una clave
- TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE
  - Algoritmos de clave permitidos: RSA_2048, RSA_3072, RSA_4096
  - Combinación permitida de modos de uso de las teclas: {Sign = true}, {Verify = true}
  - NOTA: {Verify = true} es la única opción válida cuando se importa una clave destinada a la firma, como un certificado raíz, un certificado intermedio o un certificado de firma TR-34.
- TR31_K3_ASYMMETRIC_KEY_FOR_KEY_AGREEMENT
  - Se utiliza para algoritmos de acuerdo de claves, como el ECDH

  - Algoritmos clave permitidos: ECC_NIST_P256, ECC_NIST_P384, ECC_NIST_P521
  - Combinación permitida de modos de uso clave: {= true}. DeriveKey
  - NOTA: DeriveKeyUsage se usa para especificar qué tipo de clave se derivará de esta clave base. Esto se fija en la clave creation/import.
- TR31_K2_TR34_ASYMMETRIC_KEY
  - Clave asimétrica utilizada para mecanismos de intercambio de claves compatibles, como X9.24 TR-34
  - Algoritmos clave permitidos: RSA_2048, RSA_3072, RSA_4096
  - Combinación permitida de modos de uso clave: {= true}. DeriveKey
  - Combinación permitida de modos de uso clave: {Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true}, {Encrypt = true, Wrap = true}, {Decrypt = true, Unwrap = true}, {NoRestrictions = true}
  - NOTA: {Encrypt = true, Wrap = true} es la única opción válida al importar una clave pública destinada a cifrar datos o empaquetar una clave

* Esta combinación algorithm/key de tipos no es compatible actualmente con ninguna operación criptográfica

Operaciones de datos

Una vez establecida una clave de criptografía de AWS pago, se puede utilizar para realizar operaciones criptográficas. Las distintas operaciones llevan a cabo distintos tipos de actividad, desde el cifrado y el cifrado hasta el uso de algoritmos específicos del dominio, como la generación. CVV2

Los datos cifrados no se pueden descifrar sin la clave de descifrado correspondiente (la clave simétrica o la clave privada, según el tipo de cifrado). Del mismo modo, los algoritmos de hash y los algoritmos específicos de un dominio no se pueden verificar sin la clave simétrica o la clave pública.

Para obtener información sobre los tipos de clave válidos para operaciones específicas, consulte Claves válidas para operaciones criptográficas

> **Note**
>
> Recomendamos utilizar datos de prueba en un entorno que no sea de producción. El uso de claves y datos de producción (PAN, ID de BDK, etc.) en un entorno ajeno a la producción puede afectar al ámbito de cumplimiento, por ejemplo, en el caso de PCI DSS y PCI P2PE.

Temas

- Cifrar, descifrar y volver a cifrar datos
- Generación y verificación de datos de tarjetas
- Generar, traducir y verificar los datos del PIN
- Verificar el criptograma de solicitud de autenticación (ARQC)
- Generar y verificar MAC
- Claves válidas para las operaciones criptográficas

Cifrar, descifrar y volver a cifrar datos

Los métodos de cifrado y descifrado se pueden utilizar para cifrar o descifrar datos mediante una variedad de técnicas simétricas y asimétricas, incluidas TDES, AES y RSA. Estos métodos también admiten claves derivadas mediante las técnicas DUKPT y EMV. Para los casos de uso en los que desee proteger los datos con una clave nueva sin exponer los datos subyacentes, también se puede utilizar el ReEncrypt comando.

> **Note**
>
> Al utilizar las encrypt/decrypt funciones, se supone que todas las entradas están en HexBinary; por ejemplo, un valor de 1 se introducirá como 31 (hexadecimal) y una t minúscula se representará como 74 (hexadecimal). Todas las salidas también están en hexBinary.

Para obtener más información sobre todas las opciones disponibles, consulte la Guía de la API para cifrar, descifrar y volver a cifrar.

Temas

- Cifrar datos
- Descifrado de datos

Cifrar datos

La `Encrypt Data` API se utiliza para cifrar datos mediante claves de cifrado de datos simétricas y asimétricas, así como claves derivadas de DUKPT y EMV. Se admiten varios algoritmos y variaciones, incluidos `TDES`, `RSA` y `AES`.

Las entradas principales son la clave de cifrado utilizada para cifrar los datos, los datos de texto simple en formato HexBinary que se van a cifrar y los atributos de cifrado, como el vector de inicialización y el modo para los cifrados por bloques, como el TDES. Los datos en texto plano deben estar en múltiplos de 8 bytes para`TDES`, 16 bytes para `AES` y la longitud de la clave en el caso de. `RSA` Las entradas clave simétricas (TDES, AES, DUKPT, EMV) deben rellenarse en los casos en que los datos de entrada no cumplan estos requisitos. La siguiente tabla muestra la longitud máxima del texto sin formato para cada tipo de clave y el tipo de relleno que se define para las claves RSA. `EncryptionAttributes`

Tipo de relleno	RSA_2048	RSA_3072	RSA_4096
`OAEP SHA1`	4.28	684	940
`OAEP SHA256`	380	636	892
`OAEP SHA512`	252	508	764

Tipo de relleno	RSA_2048	RSA_3072	RSA_4096
PKCS1	488	744	1 000
None	488	744	1 000

Las salidas primarias incluyen los datos encriptados como texto cifrado en formato hexBinario y el valor de la suma de comprobación de la clave de encriptación. Para obtener más información sobre todas las opciones disponibles, consulte la Guía de API para Encrypt.

Ejemplos

- Cifrar datos utilizando la clave simétrica AES
- Cifrar los datos con la clave DUKPT
- Cifre los datos mediante una clave simétrica derivada de EMV
- Cifrado de los datos utilizando una clave de RSA

Cifrar datos utilizando la clave simétrica AES

> **Note**
>
> En todos los ejemplos se asume que la clave correspondiente ya existe. Las claves se pueden crear mediante la CreateKeyoperación o importar mediante la ImportKeyoperación.

Example

En este ejemplo, cifraremos los datos en texto plano mediante una clave simétrica que se creó mediante la CreateKeyoperación o se importó mediante la operación. ImportKey Para esta operación, la clave debe estar configurada en `Encrypt` y KeyModesOfUse KeyUsage establecida en. `TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY` Consulte Claves para operaciones criptográficas para ver más opciones.

```
$ aws payment-cryptography-data encrypt-data --key-identifier arn:aws:payment-
cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi --plain-text
 31323334313233343132333431323334 --encryption-attributes 'Symmetric={Mode=CBC}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "71D7AE",
    "CipherText": "33612AB9D6929C3A828EB6030082B2BD"
}
```

Cifrar los datos con la clave DUKPT

Example

En este ejemplo, cifraremos los datos en texto plano mediante una clave DUKPT. AWS Soportes de criptografía de pagos y claves DUKPT. TDES AES Para esta operación, la clave debe estar configurada en DeriveKey y KeyModesOfUse KeyUsage configurada en. TR31_B0_BASE_DERIVATION_KEY Consulte Claves para operaciones criptográficas para ver más opciones.

```
$ aws payment-cryptography-data encrypt-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi
 --plain-text 31323334313233343132333431323334 --encryption-attributes
 'Dukpt={KeySerialNumber=FFFF9876543210E00001}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "71D7AE",
    "CipherText": "33612AB9D6929C3A828EB6030082B2BD"
}
```

Cifre los datos mediante una clave simétrica derivada de EMV

Example

En este ejemplo, cifraremos los datos de texto no cifrado mediante una clave simétrica derivada de EMV que ya se ha creado. Puede utilizar un comando como este para enviar datos a una tarjeta EMV. Para esta operación, la clave debe estar KeyModesOfUse configurada en Derive y KeyUsage establecida en TR31_E1_EMV_MKEY_CONFIDENTIALITY oTR31_E6_EMV_MKEY_OTHER. Consulte Claves para operaciones criptográficas para obtener más información.

```
$ aws payment-cryptography-data encrypt-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi
 --plain-text 33612AB9D6929C3A828EB6030082B2BD --encryption-attributes
```

```
 'Emv={MajorKeyDerivationMode=EMV_OPTION_A,PanSequenceNumber=27,PrimaryAccountNumber=1000000000
 InitializationVector=1500000000000999,Mode=CBC}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "71D7AE",
    "CipherText": "33612AB9D6929C3A828EB6030082B2BD"
}
```

Cifrado de los datos utilizando una clave de RSA

Example

En este ejemplo, cifraremos los datos en texto plano mediante una clave pública RSA que se importó mediante la operación. ImportKey Para esta operación, la clave debe estar configurada en `Encrypt` y KeyModesOfUse KeyUsage establecida en. `TR31_D1_ASYMMETRIC_KEY_FOR_DATA_ENCRYPTION` Consulte Claves para operaciones criptográficas para ver más opciones.

Para PKCS #7 u otros esquemas de relleno no admitidos actualmente, solicítelos antes de llamar al servicio y seleccione sin relleno omitiendo el indicador de relleno 'Asymmetric={}'

```
$ aws payment-cryptography-data encrypt-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/thfezpmsalcfwmsg
 --plain-text 313233343132333431323334313233343132333431323334 --encryption-attributes
 'Asymmetric={PaddingType=OAEP_SHA256}'
```

```
{
 "CipherText":
 "12DF6A2F64CC566D124900D68E8AFEAA794CA819876E258564D525001D00AC93047A83FB13 \
 E73F06329A100704FA484A15A49F06A7A2E55A241D276491AA91F6D2D8590C60CDE57A642BC64A897F4832A3930
 \
 0FAEC7981102CA0F7370BFBF757F271EF0BB2516007AB111060A9633D1736A9158042D30C5AE11F8C5473EC70F067
 \
 72590DEA1638E2B41FAE6FB1662258596072B13F8E2F62F5D9FAF92C12BB70F42F2ECDCF56AADF0E311D4118FE3591
 \
 FB672998CCE9D00FFFE05D2CD154E3120C5443C8CF9131C7A6A6C05F5723B8F5C07A4003A5A6173E1B425E2B5E42AD
 \
 7A2966734309387C9938B029AFB20828ACFC6D00CD1539234A4A8D9B94CDD4F23A",
 "KeyArn": "arn:aws:payment-cryptography:us-east-1:111122223333:key/5dza7xqd6soanjtb",
 "KeyCheckValue": "FF9DE9CE"
}
```

Descifrado de datos

La `Decrypt Data` API se utiliza para descifrar datos mediante claves de cifrado de datos simétricas y asimétricas, así como claves derivadas de DUKPT y EMV. Se admiten varios algoritmos y variaciones, incluidos `TDES`, `RSA` y `AES`.

Las entradas principales son la clave de descifrado utilizada para descifrar los datos, los datos del texto cifrado en formato hexBinario que deben descifrarse y los atributos de descifrado, como el vector de inicialización, el modo como los cifradores de bloques, etc. Las salidas principales incluyen los datos descifrados como texto plano en formato hexBinario y el valor de la suma de comprobación de la clave de descifrado. Para obtener más información sobre todas las opciones disponibles, consulte la Guía de API para descifrar.

Ejemplos

- Descifrar los datos mediante la clave simétrica AES
- Descifrar los datos con la clave DUKPT
- Descifre los datos mediante una clave simétrica derivada de EMV
- Descifrar datos con una clave de RSA

Descifrar los datos mediante la clave simétrica AES

Example

En este ejemplo, descifraremos los datos de texto cifrado mediante una clave simétrica. En este ejemplo se muestra una AES clave, pero también TDES_2KEY se admiten. TDES_3KEY Para esta operación, la clave debe estar KeyModesOfUse configurada en Decrypt y KeyUsage establecida enTR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY. Consulte Claves para operaciones criptográficas para ver más opciones.

```
$ aws payment-cryptography-data decrypt-data --key-identifier arn:aws:payment-
cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi --cipher-text
 33612AB9D6929C3A828EB6030082B2BD --decryption-attributes 'Symmetric={Mode=CBC}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "71D7AE",
    "PlainText": "313233343132333431323334313233343"
}
```

Descifrar los datos con la clave DUKPT

> **Note**
>
> El uso del descifrado de datos con DUKPT para las transacciones P2PE puede devolver a su aplicación el PAN de la tarjeta de crédito y otros datos del titular de la tarjeta que deberán tenerse en cuenta a la hora de determinar su alcance PCI DSS.

Example

En este ejemplo, descifraremos los datos de texto cifrado mediante una clave DUKPT que se creó mediante la CreateKeyoperación o se importó mediante la operación. ImportKey Para esta operación, la clave debe estar establecida en y KeyModesOfUse configurada en. `DeriveKey` KeyUsage `TR31_B0_BASE_DERIVATION_KEY` Consulte Claves para operaciones criptográficas para ver más opciones. Cuando se utiliza `DUKPT`, como algoritmo `TDES`, la longitud de los datos del texto cifrado debe ser un múltiplo de 16 bytes. Para el algoritmo `AES`, la longitud de los datos del texto cifrado debe ser un múltiplo de 32 bytes.

```
$ aws payment-cryptography-data decrypt-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi
 --cipher-text 33612AB9D6929C3A828EB6030082B2BD --decryption-attributes
 'Dukpt={KeySerialNumber=FFFF9876543210E00001}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "71D7AE",
    "PlainText": "31323334313233343132333431323334"
}
```

Descifre los datos mediante una clave simétrica derivada de EMV

Example

En este ejemplo, descifraremos los datos de texto cifrado mediante una clave simétrica derivada de EMV que se creó mediante la operación o se importó mediante la operación. CreateKeyImportKey Para esta operación, la clave debe estar establecida en y KeyModesOfUse establecida en o. `Derive` KeyUsage `TR31_E1_EMV_MKEY_CONFIDENTIALITY` `TR31_E6_EMV_MKEY_OTHER` Consulte Claves para operaciones criptográficas para obtener más información.

```
$ aws payment-cryptography-data decrypt-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi
 --cipher-text 33612AB9D6929C3A828EB6030082B2BD --decryption-attributes
 'Emv={MajorKeyDerivationMode=EMV_OPTION_A,PanSequenceNumber=27,PrimaryAccountNumber=1000000000
 InitializationVector=1500000000000999,Mode=CBC}'
```

```
{
"KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi",
"KeyCheckValue": "71D7AE",
"PlainText": "31323334313233343132333431323334"
}
```

Descifrar datos con una clave de RSA

Example

En este ejemplo, descifraremos los datos de texto cifrado mediante un par de claves RSA que se creó mediante la operación. CreateKey Para esta operación, la clave debe estar configurada como `Decrypt` habilitada y KeyModesOfUse configurada como. KeyUsage `TR31_D1_ASYMMETRIC_KEY_FOR_DATA_ENCRYPTION` Consulte Claves para operaciones criptográficas para ver más opciones.

Para PKCS #7 u otros esquemas de relleno no admitidos actualmente, seleccione sin relleno omitiendo el indicador de relleno 'Asymmetric={}' y elimine el relleno después de llamar al servicio.

```
$ aws payment-cryptography-data decrypt-data \
        --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/5dza7xqd6soanjtb --cipher-text
 8F4C1CAFE7A5DEF9A40BEDE7F2A264635C... \
        --decryption-attributes 'Asymmetric={PaddingType=OAEP_SHA256}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-
east-1:111122223333:key/5dza7xqd6soanjtb",
    "KeyCheckValue": "FF9DE9CE",
    "PlainText": "313233343132333431323334313233343132333431323334"
}
```

Generación y verificación de datos de tarjetas

Generar y verificar los datos de la tarjeta incorpora datos derivados de los datos de la tarjeta, por ejemplo CVV CVV2, CVC y DCVV.

Temas

- Generar datos de tarjetas
- Comprobación de datos de tarjetas

Generar datos de tarjetas

La `Generate Card Data` API se utiliza para generar datos de tarjetas mediante algoritmos como CVV o Dynamic. CVV2 CVV2 Para ver qué claves se pueden usar para este comando, consulte la sección Claves válidas para operaciones criptográficas.

Muchos valores criptográficos, como el CVV, CVV2 el CVV o el CVV V7, utilizan el mismo algoritmo criptográfico, pero varían los valores de entrada. Por ejemplo, CardVerificationValue1 tiene entradas como el número de tarjeta y la fecha de caducidad ServiceCode. Si bien CardVerificationValue2 solo tiene dos de estas entradas, esto se debe a que para CVV2/CVC2, el ServiceCode está fijado en 000. Del mismo modo, para iCVV, el valor ServiceCode se fija en 999. Algunos algoritmos pueden reutilizar los campos existentes, como el CAVV V8, en cuyo caso tendrá que consultar el manual del proveedor para obtener los valores de entrada correctos.

> **Note**
>
> La fecha de caducidad debe introducirse en el mismo formato (por ejemplo, MMYY o YYMM) para que la generación y la validación arrojen resultados correctos.

Generar CVV2

Example

En este ejemplo, generaremos un CVV2 para un PAN determinado con entradas de la fecha de PAN caducidad de la tarjeta. Esto supone que se ha generado una clave de verificación de la tarjeta.

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue2={CardExpiryDate=0123}
```

```
  {
      "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
      "KeyCheckValue": "CADDA1",
      "ValidationData": "801"
  }
```

Genera iCVV

Example

En este ejemplo, generaremos un iCVV para un PAN determinado con entradas dePAN, un código de servicio 999 y una fecha de caducidad de la tarjeta. Esto supone que se ha generado una clave de verificación de la tarjeta.

Para ver todos los parámetros disponibles, consulta el apartado CardVerificationValue1 de la guía de referencia de la API.

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue1='{CardExpiryDate=1127,ServiceCode=999}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "CADDA1",
    "ValidationData": "801"
}
```

Comprobación de datos de tarjetas

`Verify Card Data` se utiliza para verificar los datos que se han creado mediante algoritmos de pago que se basan en principios de cifrado, como `DISCOVER_DYNAMIC_CARD_VERIFICATION_CODE`.

Los valores de entrada suelen proporcionarse como parte de una transacción entrante a un emisor o a un socio de plataforma de apoyo. Para verificar un criptograma ARQC (utilizado para tarjetas con chips EMV), consulte Verificar el ARQC.

Para obtener más información, consulte VerifyCardValidationDatala guía de la API.

Si se verifica el valor, la API devolverá http/200. Si no se verifica el valor, devolverá http/400.

Verifica CVV2

Example

En este ejemplo, validaremos un CVV/ CVV2 para un PAN determinado. Por lo general, CVV2 lo proporciona el titular de la tarjeta o el usuario durante el momento de la transacción para su validación. Para validar su entrada, se proporcionarán los siguientes valores durante el tiempo de ejecución: la clave que se utilizará para la validación (CVK) y la fecha de caducidad de la tarjetaPAN, y CVV2 se ingresarán. El formato de caducidad de la tarjeta debe coincidir con el utilizado en la generación del valor inicial.

Para ver todos los parámetros disponibles, consulte el CardVerificationValueapartado 2 de la guía de referencia de la API.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi
 --primary-account-number=171234567890123 --verification-attributes
 CardVerificationValue2={CardExpiryDate=0123} --validation-data 801
```

```
  {
      "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
      "KeyCheckValue": "CADDA1"
  }
```

Verifica el iCVV

Example

En este ejemplo, verificaremos un iCVV para un PAN determinado con las entradas de la clave que se utilizará para la validación (CVK), un código de servicio 999PAN, la fecha de caducidad de la tarjeta y el iCVV proporcionado por la transacción para la validación.

El iCVV no es un valor introducido por el usuario (por ejemplo CVV2), sino que está incrustado en una tarjeta EMV. Se debe tener en cuenta si siempre debe validarse cuando se proporciona.

Para ver todos los parámetros disponibles, consulte el apartado CardVerificationValue1 de la guía de referencia de la API.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/tqv5yij6wtxx64pi
 --primary-account-number=171234567890123 --verification-attributes
 CardVerificationValue1='{CardExpiryDate=1127,ServiceCode=999} --validation-data 801
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "CADDA1",
    "ValidationData": "801"
}
```

Generar, traducir y verificar los datos del PIN

Las funciones de datos PIN permiten generar códigos PIN al azar, valores de verificación de números PIN (PVV) y validar los pines entrantes cifrados comparándolos con valores PVV o compensaciones de PIN.

La traducción de pines permite convertir un pin de una clave funcional a otra sin exponer el pin en texto claro, tal y como se especifica en el requisito 1 del PIN PCI.

> **Note**
>
> Como la generación y la validación del PIN suelen ser funciones del emisor y la traducción del PIN es una función típica del adquirente, recomendamos que considere el acceso con menos privilegios y establezca las políticas adecuadas para el caso de uso de su sistema.

Temas

- Traducir datos PIN
- Generar datos PIN
- Comprobación de datos PIN

Traducir datos PIN

Las funciones de traducir datos PIN se utilizan para traducir los datos PIN cifrados de un conjunto de claves a otro sin que los datos cifrados salgan del HSM. Se utiliza para el cifrado P2PE, en el que las claves de trabajo deberían cambiar, pero el sistema de procesamiento no necesita descifrar los datos o no está autorizado a hacerlo. Las entradas principales son los datos cifrados, la clave de cifrado utilizada para cifrar los datos y los parámetros utilizados para generar los valores de entrada. El otro conjunto de entradas son los parámetros de salida solicitados, como la clave que se utilizará para cifrar la salida y los parámetros que se utilizarán para crear esa salida. Las salidas principales son un conjunto de datos recién cifrado, así como los parámetros utilizados para generarlo.

> **Note**
>
> Para cumplir con la normativa PCI, los PrimaryAccountNumber valores de entrada y salida deben coincidir. No está permitido traducir un PIN de un PAN a otro.

Temas

- PIN de PEK a DUKPT
- PIN de PEK a PEK

PIN de PEK a DUKPT

Example

En este ejemplo, traduciremos un PIN de un bloque AES ISO 4 PIN usando el cifrado DUKPT a PEK TDES usando un bloque ISO 0 PIN. Esto es habitual cuando un terminal de pago cifra un PIN en ISO 4 y, después, puede volver a traducirlo al TDES para su procesamiento posterior si la siguiente conexión aún no admite el AES.

```
$ aws payment-cryptography-data translate-pin-data --encrypted-pin-block
 "AC17DC148BDA645E" --outgoing-translation-
attributes=IsoFormat0='{PrimaryAccountNumber=171234567890123}' --outgoing-
key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt  --incoming-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/4pmyquwjs3yj4vwe --incoming-translation-attributes
 IsoFormat4="{PrimaryAccountNumber=171234567890123}" --incoming-dukpt-attributes
 KeySerialNumber="FFFF9876543210E00008"
```

```
    {
            "PinBlock": "1F4209C670E49F83E75CC72E81B787D9",
            "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
            "KeyCheckValue": "7CC9E2"
        }
```

PIN de PEK a PEK

Example

En este ejemplo, traducimos un PIN cifrado con un PEK (clave de cifrado PIN) a otro PEK. Esto se suele utilizar para enrutar transacciones entre diferentes sistemas o socios que utilizan diferentes claves de cifrado y, al mismo tiempo, se mantiene el cumplimiento del PIN PCI al mantener el PIN cifrado durante todo el proceso. En este ejemplo, ambas claves utilizan el cifrado TDES de 3 claves, pero hay una variedad de opciones disponibles, que incluyen AES ISO-4 a TDES ISO-0, DUKPT a PEK o PEK. AS2805

```
$ aws payment-cryptography-data translate-pin-data --encrypted-pin-block
 "AC17DC148BDA645E" \
    --incoming-translation-attributes
 IsoFormat0='{PrimaryAccountNumber=171234567890123}' \
    --incoming-key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt \
    --outgoing-translation-attributes
 IsoFormat0='{PrimaryAccountNumber=171234567890123}' \
    --outgoing-key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh
```

```
{
    "PinBlock": "E8F2A6C4D1B93E7F",
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh",
    "KeyCheckValue": "9A325B"
}
```

El bloque PIN de salida ahora está cifrado con el segundo PEK y se puede transmitir de forma segura al sistema descendente que contiene la clave correspondiente.

Generar datos PIN

Las funciones de generación de datos PIN se utilizan para generar valores relacionados con el PIN, como el PVV y las compensaciones de bloques de pines que se utilizan para validar la introducción de los PIN por parte de los usuarios durante el tiempo de transacción o autorización. Esta API también puede generar un nuevo pin al azar mediante varios algoritmos.

Genera un PIN aleatorio y un Visa PVV correspondiente

Example

En este ejemplo, generaremos un nuevo pin (aleatorio) donde las salidas serán cifradas `PIN block` (PinData. PinBlock) y un PVV (pinData.Offset). Las entradas clave son PAN, `Pin Verification Key`, `Pin Encryption Key` y `PIN block format`.

Este comando requiere que la clave sea de tipo. `TR31_V2_VISA_PIN_VERIFICATION_KEY`

```
$ aws payment-cryptography-data generate-pin-data --generation-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2 --encryption-
key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/ivi5ksfsuplneuyt
 --primary-account-number 171234567890123 --pin-block-format ISO_FORMAT_0 --generation-
attributes VisaPin={PinVerificationKeyIndex=1}
```

```
{
            "GenerationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
            "GenerationKeyCheckValue": "7F2363",
            "EncryptionKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt",
            "EncryptionKeyCheckValue": "7CC9E2",
            "EncryptedPinBlock": "AC17DC148BDA645E",
            "PinData": {
                "VerificationValue": "5507"
            }
        }
```

Genera una Visa PVV para un pin conocido

Example

En este ejemplo, generaremos un PVV para un pin determinado (cifrado). Un PIN cifrado se puede recibir en sentido ascendente, por ejemplo, desde un terminal de pago o desde el titular de una tarjeta, utilizando el flujo de pines seleccionable por el usuario. Las entradas clave sonPAN, la `Pin Verification KeyPin Encryption Key`, la y la`Encrypted Pin Block`. `PIN block format`

```
$ aws payment-cryptography-data generate-pin-data --generation-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2
 --encryption-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt --primary-account-number
 171234567890123 --pin-block-format ISO_FORMAT_0 --generation-attributes
 VisaPinVerificationValue={PinVerificationKeyIndex=1,EncryptedPinBlock=AA584CED31790F37}
```

```
{
            "GenerationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
            "GenerationKeyCheckValue": "7F2363",
            "EncryptionKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt",
            "EncryptionKeyCheckValue": "7CC9E2",
            "EncryptedPinBlock": "AC17DC148BDA645E",
            "PinData": {
                "VerificationValue": "5507"
            }
        }
```

Genera el desfase de un IBM3624 pin para un pin

El IBM 3624 PIN Offset también se denomina a veces método IBM. Este método genera un natural/intermediate PIN utilizando los datos de validación (normalmente el PAN) y una clave PIN (PVK). Los pines naturales son, en efecto, un valor derivado y, al ser deterministas, son muy eficientes de manejar para el emisor, ya que no es necesario almacenar los datos del pin a nivel del titular de la tarjeta. La desventaja más obvia es que este esquema no tiene en cuenta los pines aleatorios o seleccionables por el titular de la tarjeta. Para permitir esos tipos de pines, se agregó un algoritmo de compensación al esquema. El desplazamiento representa la diferencia entre el pin seleccionado por el usuario (o al azar) y la clave natural. El emisor o el procesador de la tarjeta almacenan el valor de

compensación. En el momento de la transacción, el servicio de criptografía de AWS pagos recalcula internamente el pin natural y aplica la compensación para encontrarlo. A continuación, lo compara con el valor proporcionado por la autorización de la transacción.

Existen varias opciones para IBM3624:

- `Ibm3624NaturalPin`generará el pin natural y un bloque de pines cifrado
- `Ibm3624PinFromOffset`generará un bloque de pines cifrado con un desfase
- `Ibm3624RandomPin`generará un pin aleatorio y, a continuación, el bloque de pines cifrado y desplazado correspondiente.
- `Ibm3624PinOffset`genera el desfase del pin dado el pin seleccionado por el usuario.

Dentro de la criptografía de AWS pagos, se llevan a cabo los siguientes pasos:

- Rellene el panel proporcionado hasta 16 caracteres. Si se proporcionan <16, rellene en el lado derecho con el carácter de relleno proporcionado.
- Cifra los datos de validación mediante la clave de generación del PIN.
- Decimalice los datos cifrados mediante la tabla de decimalización. Esto asigna dígitos hexadecimales a dígitos decimales, por ejemplo, «A» puede asignarse a 9 y 1 puede asignarse a 1.
- Obtenga los primeros 4 dígitos de una representación hexadecimal de la salida. Este es el pin natural.
- Si el usuario seleccionó un pin o se generó de forma aleatoria, resta el pin natural del pin del cliente. El resultado es el desfase del pin.

Ejemplos

- Ejemplo: generar un desfase entre IBM3624 polos para un polo

Ejemplo: generar un desfase entre IBM3624 polos para un polo

En este ejemplo, generaremos un nuevo pin (aleatorio) donde las salidas serán cifradas `PIN block` (PinData. PinBlock) y un valor de `IBM3624` compensación (pinData.Offset). Las entradas son los `PAN` datos de validación (normalmente la panorámica), el carácter de relleno, el`Pin Verification Key`, el y el. `Pin Encryption Key` `PIN block format`

Este comando requiere que la clave de generación del pin sea del tipo `TR31_V1_IBM3624_PIN_VERIFICATION_KEY` y la clave de cifrado sea del tipo `TR31_P0_PIN_ENCRYPTION_KEY`

Example

El siguiente ejemplo muestra cómo se genera un pin aleatorio y, a continuación, se genera el bloque de pines cifrado y el valor de IBM3624 compensación mediante Ibm3624 RandomPin

```
$ aws payment-cryptography-data generate-pin-data --generation-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2
 --encryption-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt --primary-account-number
 171234567890123 --pin-block-format ISO_FORMAT_0 --generation-attributes
 Ibm3624RandomPin="{DecimalizationTable=9876543210654321,PinValidationDataPadCharacter=D,PinVal
```

```
{
             "GenerationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
             "GenerationKeyCheckValue": "7F2363",
             "EncryptionKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt",
             "EncryptionKeyCheckValue": "7CC9E2",
             "EncryptedPinBlock": "AC17DC148BDA645E",
             "PinData": {
                 "PinOffset": "5507"
             }
         }
```

Comprobación de datos PIN

Las funciones de comprobación de datos PIN se utilizan para comprobar si un PIN es correcto. Por lo general, esto implica comparar el valor del PIN previamente almacenado con el que ingresó el titular de la tarjeta en un POI. Estas funciones comparan dos valores sin exponer el valor subyacente de ninguna de las fuentes.

Valide el PIN cifrado mediante el método PVV

Example

En este ejemplo, validaremos un PIN para un PAN determinado. Por lo general, el titular de la tarjeta o el usuario proporcionan el PIN durante el momento de la transacción para su validación y se compara con el valor registrado (la entrada del titular de la tarjeta se proporciona como un valor cifrado del terminal u otro proveedor principal). Para validar esta entrada, también se proporcionarán los siguientes valores en tiempo de ejecución: la clave utilizada para cifrar el pin de entrada (que suele ser un`IWK`) PAN y el valor con el que realizar la verificación (a o). `PVV` `PIN offset`

Si la criptografía de AWS pago puede validar el PIN, se devuelve un http/200. Si el pin no está validado, devolverá un http/400.

```
$ aws payment-cryptography-data verify-pin-data --verification-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2 --encryption-
key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/ivi5ksfsuplneuyt
 --primary-account-number 171234567890123 --pin-block-format ISO_FORMAT_0  --
verification-attributes VisaPin="{PinVerificationKeyIndex=1,VerificationValue=5507}" --
encrypted-pin-block AC17DC148BDA645E
```

```
        {
            "VerificationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
            "VerificationKeyCheckValue": "7F2363",
            "EncryptionKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt",
            "EncryptionKeyCheckValue": "7CC9E2",

        }
```

Valide el PIN cifrado mediante el método PVV: error: pin incorrecto

Example

En este ejemplo, intentaremos validar un PIN para un PAN determinado, pero fallará porque el PIN es incorrecto.

Al usarlo SDKs, aparece como {"Mensaje» :"No se pudo verificar el bloqueo del PIN». , «Reason» :"INVALID_PIN "}

```
$ aws payment-cryptography-data verify-pin-data --verification-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2 --encryption-
key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/ivi5ksfsuplneuyt
 --primary-account-number 171234567890123 --pin-block-format ISO_FORMAT_0  --
verification-attributes VisaPin="{PinVerificationKeyIndex=1,VerificationValue=9999}" --
encrypted-pin-block AC17DC148BDA645E
```

```
       An error occurred (VerificationFailedException) when calling the VerifyPinData
 operation: Pin block verification failed.
```

Valide el PIN cifrado mediante el método PVV; se produce un error al introducir datos erróneos

Example

En este ejemplo, intentaremos validar un PIN para un PAN determinado, pero fallará debido a una entrada incorrecta y a que los datos entrantes no eran un PIN válido. Las causas más comunes son: 1 tecla incorrecta 2 parámetros de entrada, como el formato panorámico o de bloque de pines, son incorrectos o 3 el bloque de pines está dañado.

```
$ aws payment-cryptography-data verify-pin-data --verification-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2
 --encryption-key-identifier  --primary-account-number 171234567890123
 --pin-block-format ISO_FORMAT_0  --verification-attributes
 VisaPin="{PinVerificationKeyIndex=1,VerificationValue=9999}" --encrypted-pin-block
 AC17DC148BDA645E
```

```
       An error occurred (ValidationException) when calling the VerifyPinData
operation: Pin block provided is invalid. Please check your input to ensure all field
values are correct.
```

Valide un PIN comparándolo con el desfase de pin almacenado anteriormente IBM3624

En este ejemplo, validaremos el PIN proporcionado por el titular de la tarjeta con la diferencia de pin almacenada en el archivo del emisor o procesador de la tarjeta. Las entradas son similares a ??? las del PIN cifrado adicional que proporciona el terminal de pago (u otro proveedor previo, como la red de tarjetas). Si el pin coincide, la API devolverá http 200., donde las salidas serán cifradas `PIN block` (. PinData PinBlock) y un valor de `IBM3624` compensación (pINData.Offset).

Este comando requiere que la clave de generación del pin sea de tipo `TR31_V1_IBM3624_PIN_VERIFICATION_KEY` y la clave de cifrado sea de tipo `TR31_P0_PIN_ENCRYPTION_KEY`

Example

```
$ aws payment-cryptography-data generate-pin-data --generation-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2
 --encryption-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt --primary-account-number
 171234567890123 --pin-block-format ISO_FORMAT_0 --generation-attributes
 Ibm3624RandomPin="{DecimalizationTable=9876543210654321,PinValidationDataPadCharacter=D,PinVal
```

```
{
"GenerationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
"GenerationKeyCheckValue": "7F2363",
"EncryptionKeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
"EncryptionKeyCheckValue": "7CC9E2",
"EncryptedPinBlock": "AC17DC148BDA645E",
"PinData": {
  "PinOffset": "5507"
}
}
```

Verificar el criptograma de solicitud de autenticación (ARQC)

La API de verificación del criptograma de solicitud de autenticación se utiliza para verificar el ARQC. La generación del ARQC está fuera del alcance de la criptografía de AWS pagos y, por lo general, se realiza en una tarjeta con chip EMV (o un equivalente digital, como una billetera móvil) durante el tiempo de autorización de la transacción. Un ARQC es único para cada transacción y su objetivo es mostrar criptográficamente la validez de la tarjeta y garantizar que los datos de la transacción coincidan exactamente con los de la transacción actual (esperada).

AWS La criptografía de pagos ofrece una variedad de opciones para validar el ARQC y generar valores ARPC opcionales, incluidos los definidos en la EMV 4.4, libro 2, y otros esquemas utilizados por Visa y Mastercard. Para obtener una lista completa de todas las opciones disponibles, consulte la sección de la VerifyCardValidationData Guía de API.

Los criptogramas ARQC suelen requerir las siguientes entradas (aunque esto puede variar según la implementación):

- PAN: se especifica en el campo PrimaryAccountNumber

- Número de secuencia PAN (PSN): especificado en el campo PanSequenceNumber
- Método de derivación de claves, como la clave de sesión común (CSK), especificado en el SessionKeyDerivationAttributes
- Modo de derivación de clave maestra (como la opción A de EMV): especificado en el MajorKeyDerivationMode
- Datos de la transacción: una cadena de varios datos de transacciones, terminales y tarjetas, como el importe y la fecha, especificados en el campo TransactionData
- Clave maestra del emisor: la clave maestra utilizada para derivar la clave de criptograma (AC) utilizada para proteger las transacciones individuales y especificada en el campo KeyIdentifier

Temas

- Creación de datos de transacciones
- Relleno de datos de transacciones
- Ejemplos

Creación de datos de transacciones

El contenido (y el orden) exactos del campo de datos de la transacción varían según la implementación y el esquema de red, pero los campos mínimos recomendados (y la secuencia de concatenación) se definen en la sección 8.1.1 del libro 2 de EMV 4.4: Selección de datos. Si los tres primeros campos son importe (17.00), otro importe (0,00) y país de compra, los datos de la transacción comenzarán de la siguiente manera:

- 000000001700 - cantidad: 12 posiciones implican un decimal de dos dígitos
- 000000000000 - otra cantidad: 12 posiciones implican un decimal de dos dígitos
- 0124: código de país de cuatro dígitos
- Datos de transacción de salida (parciales): 00000000170000000000000000124

Relleno de datos de transacciones

Los datos de las transacciones deben rellenarse antes de enviarlos al servicio. La mayoría de los esquemas utilizan el relleno ISO 9797 Método 2, en el que se añade una cadena hexadecimal 80 seguida de 00 hasta que el campo es un múltiplo del tamaño del bloque de cifrado; 8 bytes o

16 caracteres para TDES y 16 bytes o 32 caracteres para AES. La alternativa (método 1) no es tan común pero utiliza sólo 00 como caracteres de relleno.

Relleno ISO 9797 Método 1

Sin relleno:
0000000017000000000000000840008000800008401605170000000093800000B03011203
(74 caracteres o 37 bytes)

Con relleno:
0000000017000000000000000840008000800008401605170000000093800000B03011203000000
(80 caracteres o 40 bytes)

Relleno ISO 9797 Método 2

Sin relleno:
0000000017000000000000000840008000800008401605170000000093800000B1F220103000000
(80 caracteres o 40 bytes)

Sin relleno:
0000000017000000000000000840008000800008401605170000000093800000B1F220103000008000000
(88 caracteres o 44 bytes)

Ejemplos

Visa CVN10

Example

En este ejemplo, validaremos un ARQC generado con Visa. CVN10

Si la criptografía de AWS pagos puede validar el ARQC, se devuelve un http/200. Si, entonces, el ARCQ (criptograma de solicitud de autorización) no está validado, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-auth-request-cryptogram --auth-request-
cryptogram D791093C8A921769 \
--key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk \
--major-key-derivation-mode EMV_OPTION_A \
--transaction-data
 00000000170000000000000008400080008000084016051700000000093800000B03011203000000 \
--session-key-derivation-attributes='{"Visa":{"PanSequenceNumber":"01" \
,"PrimaryAccountNumber":"9137631040001422"}}'
```

```
{
  "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk",
  "KeyCheckValue": "08D7B4"
}
```

Visa y Visa CVN18 CVN22

Example

En este ejemplo, validaremos un ARQC generado con Visa CVN18 o. CVN22 Las operaciones criptográficas son las mismas entre CVN18 y, sin CVN22 embargo, los datos contenidos en los datos de las transacciones varían. En comparación con CVN10, se genera un criptograma completamente diferente incluso con las mismas entradas.

Si la criptografía de AWS pagos es capaz de validar el ARQC, se devuelve un http/200. Si el ARCQ no está validado, devolverá un http/400.

```
$ aws payment-cryptography-data verify-auth-request-cryptogram \
--auth-request-cryptogram 61EDCC708B4C97B4
--key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk \
--major-key-derivation-mode EMV_OPTION_A
--transaction-data
 00000000170000000000000084000800080000840160517000000000093800000B1F22010300000000000
 \
00000000000000000000000000000000000000000800000000000000
--session-key-derivation-attributes='{"EmvCommon":
{"ApplicationTransactionCounter":"000B", \
"PanSequenceNumber":"01","PrimaryAccountNumber":"9137631040001422"}}'
```

```
{
  "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk",
  "KeyCheckValue": "08D7B4"
}
```

Generar y verificar MAC

Los códigos de autenticación de mensajes (MAC) se utilizan normalmente para autentificar la integridad de un mensaje (independientemente de si se ha modificado). Los hashes criptográficos, como el HMAC (código de autenticación de Hash-Based mensajes) CBC-MAC y el CMAC (código de autenticación de Cipher-based mensajes), proporcionan una seguridad adicional para el remitente del MAC mediante el uso de la criptografía. El HMAC se basa en funciones de hash, mientras que el CMAC se basa en cifrados por bloques. El servicio también es compatible con los algoritmos ISO9797 1 y 3, que son tipos de. CBC-MACs

Todos los algoritmos MAC de este servicio combinan una función hash criptográfica y una clave secreta compartida. Reciben un mensaje y una clave secreta, como el material clave de una llave, y devuelven una etiqueta o mac únicos. Si cambia incluso un carácter del mensaje, o si la clave secreta cambia, la etiqueta resultante es totalmente diferente. Al requerir una clave secreta, los MAC criptográficos también proporcionan autenticación; es imposible generar una mac idéntica sin la clave secreta. Los MAC criptográficos a veces se llaman firmas simétricas, porque funcionan como firmas digitales, pero utilizan una única clave para la firma y la verificación.

AWS La criptografía de pagos admite varios tipos de MAC:

ALGORITMO 1 ISO9797

Denotado por ISO9797_ALGORITHM1`KeyUsage`. Si el campo no es un múltiplo del tamaño de un bloque (8 caracteres bytes/16 hexadecimales para el TDES y 16 bytes/32 caracteres para el AES), Payment Cryptography aplicará automáticamente el método de relleno 1 según la norma ISO9797. AWS Si necesita otros métodos de relleno, puede aplicarlos antes de llamar al servicio.

ALGORITMO 3 ISO9797 (MAC minorista)

Denotado por `KeyUsage` ISO9797_ALGORITHM3. Se aplican las mismas reglas de relleno que en el Algoritmo 1

ALGORITMO 5 ISO9797 (CMAC)

Denotado por `KeyUsage` del TR31_M6_ISO_9797_5_CMAC_KEY

HMAC

Denotado por `KeyUsage` del TR31_M7_HMAC_KEY incluyendo HMAC_SHA224, HMAC_SHA256, HMAC_SHA384 y HMAC_SHA512

AS2805.4.1 MAC

Denotado por `KeyUsage` TR31_M0_ISO_16609_MAC_KEY. Para obtener más información sobre el AS2805, consulte ???

DUKPT MAC

El DUKPT MAC se utiliza normalmente para confirmar el origen y la carga útil de los mensajes en los terminales de pago. to/from Obtiene una clave mediante técnicas de derivación DUKPT y, a continuación, realiza el MAC. Las claves utilizadas con esta opción se indican con el símbolo TR31_B0_BASE_DERIVATION_KEY. `KeyUsage`

EMV MAC

En la documentación de EMV, la MAC suele denominarse clave de integridad. Deriva una clave mediante técnicas de derivación EMV y, a continuación, utiliza la norma ISO9797_ALGORITHM3 internamente. Por lo general, se utiliza para enviar los scripts del emisor a una tarjeta con chip para su reprogramación. Las claves utilizadas con esta opción se indican con el símbolo TR31_E2_EMV_MKEY_INTEGRITY`KeyUsage`. Si está enviando un script y actualizando un pin fuera de línea, asegúrese de que realice estas dos operaciones. GenerateMacEmvPinChange

Temas

- Generar MAC
- Verificar MAC

Generar MAC

La API Generate MAC se utiliza para autenticar los datos relacionados con las tarjetas, como rastrear los datos de una banda magnética de tarjetas, mediante el uso de claves criptográficas conocidas para generar un MAC (código de autenticación de mensajes) para la validación de los datos entre las partes remitentes y receptoras. Los datos utilizados para generar el MAC incluyen los datos de los mensajes, la clave de cifrado MAC secreta y el algoritmo MAC para generar un valor MAC único para la transmisión. La parte receptora del MAC utiliza los mismos datos del mensaje MAC, la misma clave de cifrado MAC y el mismo algoritmo para reproducir otro valor MAC con fines de comparación y autenticación de datos. Aunque cambie un carácter del mensaje o la clave MAC utilizada para la verificación no sea idéntica, el valor MAC resultante será diferente. La API admite las claves de cifrado MAC HMAC y EMV MAC (que utilizan una clave MAC estática y una clave DUKPT derivada) del algoritmo 1 de la ISO 9797-1 y el algoritmo 3 de la ISO 9797-1.

El valor de entrada para `message-data` debe ser un dato hexBinary.

Para obtener más información sobre todas las opciones de esta API, consulte y. GenerateMacVerifyMac

El parámetro opcional mac-length te permite truncar el valor de salida (aunque esto también se puede hacer dentro del código). Una longitud de 8 se refiere a 8 bytes o 16 caracteres hexadecimales.

Las claves MAC se pueden crear con criptografía AWS de pago mediante una llamada CreateKeyo importarse mediante una llamada ImportKey.

> **Note**
>
> Los algoritmos CMAC y HMAC no requieren relleno. Todos los demás requieren que los datos se rellenen hasta el tamaño de bloque del algoritmo, que es múltiplos de 8 bytes (16 caracteres hexadecimales) para el TDES y 16 bytes (32 caracteres hexadecimales) para el AES.

Ejemplos

- Genera HMAC
- Genere el MAC mediante el algoritmo ISO 9797-1 3
- Genere MAC mediante CMAC
- Genere MAC mediante DUKPT CMAC

Genera HMAC

En este ejemplo, generaremos un HMAC (código de autenticación de Hash-Based mensajes) para la autenticación de los datos de la tarjeta mediante el algoritmo HMAC `HMAC_SHA256` y la clave de cifrado HMAC. La clave debe estar KeyUsage configurada en y en. `TR31_M7_HMAC_KEY` KeyModesOfUse `Generate` La longitud del hash (por ejemplo, 256) se define cuando se crea la clave y no se puede modificar.

El parámetro opcional mac-length recortará el MAC de salida, aunque también se puede realizar fuera del servicio. Este valor está en bytes, por lo que un valor de 16 esperará una cadena hexadecimal de 32 de longitud.

Example

```
$ aws payment-cryptography-data generate-mac \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6 \
    --message-data
 "3b3130383834393030313037333934313533d32343038323236303030373030303f33" \
    --generation-attributes Algorithm=HMAC
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6",
    "KeyCheckValue": "2976E7",
    "Mac": "ED87F26E961C6D0DDB78DA5038AA2BDDEA0DCE03E5B5E96BDDD494F4A7AA470C"
}
```

Genere el MAC mediante el algoritmo ISO 9797-1 3

En este ejemplo, generaremos un MAC utilizando el algoritmo 3 de la norma ISO 9797-1 (MAC minorista) para la autenticación de los datos de las tarjetas. La clave debe estar KeyUsage configurada en `TR31_M3_ISO_9797_3_MAC_KEY` y KeyModesOfUse en. `Generate`

Example

```
$ aws payment-cryptography-data generate-mac \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h \
    --message-data
 "3b3130383834393030313037333934313533d32343038323236303030373030303f33" \
    --generation-attributes="Algorithm=ISO9797_ALGORITHM3"
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
    "KeyCheckValue": "2976EA",
    "Mac": "A8F7A73DAF87B6D0"
}
```

Genere MAC mediante CMAC

El CMAC se usa más comúnmente cuando las claves son AES, pero también es compatible con el TDES. En este ejemplo, generaremos un MAC mediante el CMAC (algoritmo 5 de la norma ISO 9797-1) para la autenticación de los datos de la tarjeta con una clave AES. La clave debe estar KeyUsage configurada en y en. `TR31_M6_ISO_9797_5_CMAC_KEY` KeyModesOfUse `Generate`

Example

```
$ aws payment-cryptography-data generate-mac \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
    --message-data
 "3b3130383834393030313037333934313533d32343038323236303030373030303f33" \
    --generation-attributes Algorithm="CMAC"
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "C1EB8F",
    "Mac": "1F8C36E63F91E4E93DF7842BF5E2E5F7"
}
```

Genere MAC mediante DUKPT CMAC

En este ejemplo, se genera una MAC mediante la DUKPT (clave única derivada por transacción) con la CMAC para la autenticación de los datos de la tarjeta. La clave debe estar KeyUsage establecida `TR31_B0_BASE_DERIVATION_KEY` y establecida en KeyModesOfUse `DeriveKey` true.

Las claves DUKPT obtienen una clave única para cada transacción mediante una clave de derivación básica (BDK) y un número de serie de la clave (KSN).

Example

```
$ aws payment-cryptography-data generate-mac --key-identifier arn:aws:payment-
cryptography:us-east-2:111122223333:key/qnobl5lghrzunce6 --message-data
 "3b3130383834393030313037333934313533d323430383232363030303730303033f33" --generation-
attributes="DukptCmac={KeySerialNumber="932A6E954ABB32DD00000001",DukptKeyVariant=BIDIRECTIONAL
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6",
    "KeyCheckValue": "C1EB8F",
    "Mac": "1F8C36E63F91E4E93DF7842BF5E2E5F7"
}
```

Verificar MAC

Verifique que la MAC API se utiliza para verificar MAC (código de autenticación de mensajes) para la autenticación de datos relacionados con tarjetas. Debe utilizar la misma clave de cifrado utilizada durante la generación del MAC para reproducir el valor MAC para la autenticación. La clave de cifrado MAC se puede crear con criptografía de AWS pago mediante una llamada CreateKeyo importarse mediante una llamada. ImportKey La API admite las claves de cifrado DUKPT MAC, HMAC y EMV MAC para esta operación.

Si el valor se verifica, el parámetro de respuesta `MacDataVerificationSuccessful` devolverá `Http/200`, en caso contrario `Http/400` con un mensaje indicando que `Mac verification failed`.

Ejemplos

- Verifica HMAC
- Verifique el MAC mediante DUKPT CMAC

Verifica HMAC

En este ejemplo, verificaremos un HMAC (código de autenticación de Hash-Based mensajes) para la autenticación de los datos de la tarjeta mediante el algoritmo HMAC `HMAC_SHA256` y la clave de cifrado HMAC. La clave debe estar KeyUsage establecida `TR31_M7_HMAC_KEY` y establecida en KeyModesOfUse `Verify` true.

Example

```
$ aws payment-cryptography-data verify-mac \
     --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6 \
     --message-data
 "3b343038383439303031303733393431353d323430383232363030303730303033f33" \
     --mac ED87F26E961C6D0DDB78DA5038AA2BDDEA0DCE03E5B5E96BDDD494F4A7AA470C \
     --verification-attributes Algorithm=HMAC_SHA256
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6",
    "KeyCheckValue": "2976E7"
}
```

Verifique el MAC mediante DUKPT CMAC

En este ejemplo, verificaremos un MAC mediante la DUKPT (clave única derivada por transacción) con la CMAC para la autenticación de los datos de la tarjeta. La clave debe estar KeyUsage establecida `TR31_B0_BASE_DERIVATION_KEY` y establecida en KeyModesOfUse `DeriveKey` true. Las claves DUKPT obtienen una clave única para cada transacción mediante una clave de derivación básica (BDK) y un número de serie de la clave (KSN). El valor de DukptKeyVariant debe coincidir entre el remitente y el destinatario. Por lo general, REQUEST se usa del terminal al servidor, VERIFY del servidor al terminal y BIDIRECTIONAL cuando se usa una sola clave en ambas direcciones.

Example

```
$ aws payment-cryptography-data verify-mac \
     --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
     --message-data
 "3b343038383439303031303733393431353d323430383232363030303730303033f33" \
     --mac D8E804EE74BF1D909A2C01C0BDE8EF34 \
     --verification-attributes
 DukptCmac='{"KeySerialNumber":"932A6E954ABB32DD00000001","DukptKeyVariant":"BIDIRECTIONAL"}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "C1EB8F"
}
```

Claves válidas para las operaciones criptográficas

Algunas claves solo se pueden utilizar para determinadas operaciones. Además, algunas operaciones pueden limitar los modos de uso de las claves. Consulte la tabla siguiente para las combinaciones permitidas.

> **Note**
>
> Ciertas combinaciones, si bien están permitidas, pueden crear situaciones inutilizables, como generar códigos CVV (`generate`) pero luego no pueden verificarlos (`verify`).

Temas

- GenerateCardData
- VerifyCardData
- GeneratePinData (para VISA/ABA esquemas)
- GeneratePinData (para) IBM3624
- VerifyPinData (para esquemas) VISA/ABA
- VerifyPinData (para) IBM3624

- Descifrado de datos
- Cifrado de datos
- Traducir datos PIN
- Generar/verificar el MAC
- GenerateMacEmvPinChange
- VerifyAuthRequestCryptogram
- Clave de Importación/Exportación
- Tipos de claves sin utilizar

GenerateCardData

Punto de conexión de la API	Operación criptográfica o algoritmo	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
GenerateCardData	• AMEX_CARD_SECURITY_CODE_VERSION_1 • AMEX_CARD_SECURITY_CODE_VERSION_2	TR31_C0_CARD_KEY_VERIFICATION_KEY	• TDES_2KEY • TDES_3KEY	{ Generate = true },{ Generate = true, Verify = true }
GenerateCardData	• CARD_VERIFICATION_VALUE_1 • CARD_VERIFICATION_VALUE_2	TR31_C0_CARD_CLAVE DE VERIFICACIÓN	• TDES_2KEY	{ Generate = true },{ Generate = true, Verify = true }
GenerateCardData	• CARDHOLDER_AUTHENTICATION_V	TR31_E6_EMV_MKEY_OTHER	• TDES_2KEY	{= verdadero} DeriveKey

Punto de conexión de la API	Operación criptográfica o algoritmo	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
	ERIFICATI ON_VALUE			
GenerateC ardData	• DYNAMIC_C ARD_VERIF ICATION_C ODE	TR31_E4_E MV_MKEY_D YNAMIC_NU MBERS	• TDES_2KEY	{= verdadero} DeriveKey
GenerateC ardData	• DYNAMIC_C ARD_VERIF ICATION_V ALUE	TR31_E6_E MV_MKEY_O THER	• TDES_2KEY	{= verdadero} DeriveKey

VerifyCardData

Operación criptográfica o algoritmo	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
• AMEX_CARD _SECURITY _CODE_VER SION_1 • AMEX_CARD _SECURITY _CODE_VER SION_2	TR31_C0_C ARD_CLAVE DE VERIFICACIÓN	• TDES_2KEY • TDES_3KEY	{ Generate = true }, { Generate = true, Verify = true }
• CARD_VERI FICATION_ VALUE_1	TR31_C0_C ARD_CLAVE DE VERIFICACIÓN	• TDES_2KEY	{ Generate = true }, { Generate = true, Verify = true }

Operación criptográfica o algoritmo	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
• CARD_VERIFICATION_VALUE_2			
• CARDHOLDER_AUTHENTICATION_VERIFICATION_VALUE	TR31_E6_EMV_MKEY_OTHER	• TDES_2KEY	{= verdadero} DeriveKey
• DYNAMIC_CARD_VERIFICATION_CODE	TR31_E4_EMV_MKEY_DYNAMIC_NUMBERS	• TDES_2KEY	{= verdadero} DeriveKey
• DYNAMIC_CARD_VERIFICATION_VALUE	TR31_E6_EMV_MKEY_OTHER	• TDES_2KEY	{= verdadero} DeriveKey

GeneratePinData (para VISA/ABA esquemas)

`VISA_PIN or VISA_PIN_VERIFICATION_VALUE`

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Clave de cifrado de PIN	TR31_P0_PIN_ENCRYPTION_KEY	• TDES_2KEY • TDES_3KEY	• { Encrypt = true, Wrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true }

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
			• {= verdadero} NoRestrictions
Clave de generación de PIN	TR31_V2_VISA_PIN_VERIFICATION_KEY	• TDES_3KEY	• { Generate = true } • { Generate = true, Verify = true }

GeneratePinData (para) **IBM3624**

`IBM3624_PIN_OFFSET,IBM3624_NATURAL_PIN,IBM3624_RANDOM_PIN, IBM3624_PIN_FROM_OFFSET)`

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Clave de cifrado de PIN	TR31_P0_PIN_ENCRYPTION_KEY	• TDES_2KEY • TDES_3KEY	Para _NATURAL_ PIN, _RANDOM_PIN, _PIN_FROM_OFFSET IBM3624 IBM3624 IBM3624 • { Encrypt = true, Wrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • NoRestrictions {= verdadero}

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
			Para IBM3624 _PIN_OFFSET • { Encrypt = true, Unwrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • {= verdadero} NoRestrictions
Clave de generación de PIN	TR31_V1_ _PIN_CLAVE DE VERIFICACIÓN IBM3624	• TDES_3KEY	• { Generate = true } • { Generate = true, Verify = true }

VerifyPinData (para esquemas) VISA/ABA

`VISA_PIN`

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Clave de cifrado de PIN	TR31_P0_P IN_ENCRYP TION_KEY	• TDES_2KEY • TDES_3KEY	• { Decrypt = true, Unwrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true }

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
			• {= verdadero} NoRestrictions
Clave de generación de PIN	TR31_V2_V ISA_PIN_VERIFICATI ON_KEY	• TDES_3KEY	• { Verify = true } • { Generate = true, Verify = true }

VerifyPinData (para) **IBM3624**

`IBM3624_PIN_OFFSET,IBM3624_NATURAL_PIN,IBM3624_RANDOM_PIN, IBM3624_PIN_FROM_OFFSET)`

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Clave de cifrado de PIN	TR31_P0_P IN_ENCRYP TION_KEY	• TDES_2KEY • TDES_3KEY	Para _NATURAL_ PIN, _RANDOM_P IN, _PIN_FROM _OFFSET IBM3624 IBM3624 IBM3624 • { Decrypt = true, Unwrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • NoRestrictions {= verdadero}
Clave de verificación de PIN	TR31_V1_ _PIN_CLAVE DE	• TDES_3KEY	• { Verify = true }

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
	VERIFICACIÓN IBM3624		• { Generate = true, Verify = true }

Descifrado de datos

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
DUKPT	TR31_B0_CLAVE DE DERIVACIÓN BASE	• TDES_2KEY • AES_128 • AES_192 • AES_256	• {= verdadero} DeriveKey • { NoRestrictions = verdadero}
EMV	TR31_E1_EMV_MKEY_CONFIDENCIALIDAD TR31_E6_EMV_MKEY_OTHER	• TDES_2KEY	• {= verdadero} DeriveKey
RSA	TR31_D1_CLAVE ASIMÉTRICA PARA EL CIFRADO DE DATOS	• RSA_2048 • RSA_3072 • RSA_4096	• { Decrypt = true, Unwrap=true} • {Encrypt=true, Wrap=true,Decrypt = true, Unwrap=true}
Claves simétricas	TR31_D0_KEY_SYMMETRIC_DATA_ENCRYPTION_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192	• {Decrypt = true, Unwrap=true} • {Encrypt=true, Wrap=true,Decrypt

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
		• AES_256	= true, Unwrap=true} • {= verdadero} NoRestrictions

Cifrado de datos

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
DUKPT	TR31_B0_BASE_CLAVE DE DERIVACIÓN	• TDES_2KEY • AES_128 • AES_192 • AES_256	• {= verdadero} DeriveKey • { NoRestrictions = verdadero}
EMV	TR31_E1_EMV_MKEY_CONFIDENCIALIDAD TR31_E6_EMV_MKEY_OTHER	• TDES_2KEY	• {= verdadero} DeriveKey
RSA	TR31_D1_CLAVE ASIMÉTRICA PARA EL CIFRADO DE DATOS	• RSA_2048 • RSA_3072 • RSA_4096	• { Encrypt = true, Wrap=true} • {Encrypt=true, Wrap=true,Decrypt = true, Unwrap=true}
Claves simétricas	TR31_D0_KEY_SYMMET	• TDES_2KEY • TDES_3KEY	• {Encrypt = true, Wrap=true}

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
	RIC_DATA_ ENCRYPTION_KEY	• AES_128 • AES_192 • AES_256	• {Encrypt=true, Wrap=true,Decrypt = true, Unwrap=true} • {= verdadero} NoRestrictions

Traducir datos PIN

Dirección	Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Origen de datos de entrada	DUKPT	TR31_B0_B ASE_CLAVE DE DERIVACIÓN	• TDES_2KEY • AES_128 • AES_192 • AES_256	• {= verdadero} DeriveKey • { NoRestrictions = verdadero}
Origen de datos de entrada	no DUKPT (PEK, AWK, IWK, etc.)	TR31_P0_P IN_ENCRYP TION_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• { Decrypt = true, Unwrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • {= verdadero} NoRestrictions

Dirección	Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Objetivo de datos de salida	DUKPT	TR31_B0_BASE_CLAVE DE DERIVACIÓN	• TDES_2KEY • AES_128 • AES_192 • AES_256	• {= verdadero} DeriveKey • { NoRestrictions = verdadero}
Objetivo de datos de salida	no DUKPT (PEK, IWK, AWK, etc)	TR31_P0_PIN_ENCRYPTION_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• { Encrypt = true, Wrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • {= verdadero} NoRestrictions

Generar/verificar el MAC

Las claves MAC se utilizan para crear hashes criptográficos de varios datos. message/body No se recomienda crear una clave con modos de uso de claves limitados, ya que no podrá realizar la operación de coincidencia. Sin embargo, puede import/export utilizar una clave con una sola operación si el otro sistema está diseñado para realizar la otra mitad del par de operaciones.

Uso permitido de claves	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Clave MAC	TR31_M1_ISO_9797_1_MAC_KEY	• TDES_2KEY • TDES_3KEY	• { Generate = true } • { Generate = true, Verify = true }

Uso permitido de claves	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
			• { Verify = true } • { Generate = true }
Clave MAC (MAC minorista)	TR31_M1_ISO_9797_3_MAC_KEY	• TDES_2KEY • TDES_3KEY	• { Generate = true } • { Generate = true, Verify = true } • { Verify = true } • { Generate = true }
Clave MAC (CMAC)	TR31_M6_ISO_9797_5_CMAC_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• { Generate = true } • { Generate = true, Verify = true } • { Verify = true } • { Generate = true }
Clave MAC (HMAC)	TR31_M7_HMAC_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• { Generate = true } • { Generate = true, Verify = true } • { Verify = true }
Tecla MAC () AS2805	TR31_M0_ISO_16609_MAC_KEY	• TDES_2KEY • TDES_3KEY	• { Generate = true } • { Generate = true, Verify = true } • { Verify = true }

GenerateMacEmvPinChange

GenerateMacEmvPinChange combina la generación de MAC y el cifrado de PIN para las operaciones de cambio de PIN fuera de línea de EMV. Esta operación requiere dos tipos de claves

diferentes: una clave de integridad para la generación de MAC y una clave de confidencialidad para el cifrado de PIN.

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Clave de integridad de mensajería segura	TR31_E2_EMV_MKEY_INTEGRITY	• TDES_2KEY	• {= verdadero} NoRestrictions
Clave de confidencialidad de mensajería segura	TR31_E1_EMV_MKEY_CONFIDENCIALITY	• TDES_2KEY	• {= verdadero} DeriveKey
PIN PEK (clave de cifrado PIN) actual	TR31_P0_PIN_ENCRYPTION_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• { Decrypt = true, Unwrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • {= verdadero} NoRestrictions
Nuevo PIN PEK (clave de cifrado PIN)	TR31_P0_PIN_ENCRYPTION_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• { Decrypt = true, Unwrap = true } • { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true } • {= verdadero} NoRestrictions
Clave ARQC	TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS	• TDES_2KEY	• {= verdadero} DeriveKey

Tipo de clave	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Note Solo se aplica a los esquemas de derivación de Visa y Amex.			

VerifyAuthRequestCryptogram

Uso permitido de claves	Opción EMV	Algoritmo clave permitido	Combinación permitida de modos de uso clave
• OPCIÓN A • OOCIÓN B	TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS	• TDES_2KEY	• {= verdadero} DeriveKey

Clave de Importación/Exportación

Operation Type (Tipo de operación)	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
Llave de embalaje TR-31	TR31_K1_KEY_BLOCK_PROTECTION_KEY	• TDES_2KEY • TDES_3KEY • AES_128 • AES_192 • AES_256	• {Encrypt = true, Wrap = true} (solo exportación) • {Decrypt = true, Unwrap = true} (solo importación)

Operation Type (Tipo de operación)	Uso permitido de claves	Algoritmo clave permitido	Combinación permitida de modos de uso clave
	TR31_K0_KEY_ENCRYPTION_KEY		• { Encrypt = true, Decrypt = true, Wrap = true, Unwrap = true }
Importación de una CA de confianza	TR31_S0_CLAVE ASIMÉTRICA PARA FIRMA DIGITAL	• RSA_2048 • RSA_3072 • RSA_4096	• { Verify = true }
Importación de un certificado de clave pública para el cifrado asimétrico	TR31_D1_A SYMMETRIC_KEY_FOR_DATA_ENCRYPTION	• RSA_2048 • RSA_3072 • RSA_4096	• {ENCRYPT= VERDADERO, WRAP=TRUE}
Clave utilizada para algoritmos de acuerdo de claves como el ECDH	TR31_K3_A SYMMETRIC_KEY_FOR_KEY_AGREEMENT	• ECC_NIST_P256 • ECC_NIST_P384 • ECC_NIST_P521	• {= verdadero} DeriveKey

Tipos de claves sin utilizar

La criptografía de AWS pagos no utiliza actualmente los siguientes tipos de claves

- TR31_P1_PIN_GENERATION_KEY

Casos de uso comunes

AWS La criptografía de pagos admite muchas operaciones criptográficas de pago típicas. Los siguientes temas sirven de guía sobre cómo usar estas operaciones en casos de uso comunes típicos. Para obtener una lista de todos los comandos, consulta la API de criptografía de AWS pagos.

Temas

- Emisores y procesadores de emisores
- Facilitadores de adquisiciones y pagos

Emisores y procesadores de emisores

Los casos de uso de los emisores suelen constar de varias partes. Esta sección está organizada por función (por ejemplo, trabajar con pines). En un sistema de producción, las llaves suelen centrarse en una bandeja de tarjetas determinada y se crean durante la configuración de la papelera y no en línea, como se muestra aquí.

Temas

- Funciones generales
- Funciones específicas de la red

Funciones generales

Temas

- Genera un pin aleatorio y el PVV asociado y, a continuación, verifica el valor
- Genera o verifica un CVV para una tarjeta determinada
- Genera o verifica una CVV2 para una tarjeta específica
- Genera o verifica un iCVV para una tarjeta específica
- Verifique un ARQC de EMV y genere un ARPC
- Genere y verifique un MAC EMV
- Genera un EMV MAC para el cambio de PIN

Genera un pin aleatorio y el PVV asociado y, a continuación, verifica el valor

Temas

- Crea la (s) clave (s)
- Genera un pin aleatorio, genera el PVV y devuelve el PIN y el PVV cifrados
- Valide el PIN cifrado mediante el método PVV

Crea la (s) clave (s)

Para generar un pin aleatorio y el PVV, necesitarás dos claves: una clave de verificación del PIN (PVK) para generar el PVV y una clave de cifrado del PIN para cifrar el pin. El pin en sí se genera aleatoriamente de forma segura dentro del servicio y no está relacionado criptográficamente con ninguna de las claves.

El PGK debe ser una clave del algoritmo TDES_2KEY basado en el propio algoritmo PVV. Un PEK puede ser TDES_2KEY, TDES_3KEY o AES_128. En este caso, dado que el PEK está diseñado para uso interno en el sistema, el AES_128 sería una buena opción. Si un PEK se utiliza para intercambiarlo con otros sistemas (p. ej., redes de tarjetas, compradores ATMs) o se va a trasladar como parte de una migración, TDES_2KEY puede ser la opción más adecuada por motivos de compatibilidad.

Cree el PEK

```
$ aws payment-cryptography create-key \
               --exportable
               --key-attributes
 KeyAlgorithm=AES_128,KeyUsage=TR31_P0_PIN_ENCRYPTION_KEY,\
                   KeyClass=SYMMETRIC_KEY,\
                   KeyModesOfUse='{Encrypt=true,Decrypt=true,Wrap=true,Unwrap=true}' --
tags='[{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
               "Key": {
                   "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
                   "KeyAttributes": {
```

```
                    "KeyUsage": "TR31_P0_PIN_ENCRYPTION_KEY",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "AES_128",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": true,
                        "Sign": false,
                        "Verify": true,
                        "DeriveKey": false,
                        "NoRestrictions": false
                    }
                },
                "KeyCheckValue": "7CC9E2",
                "KeyCheckValueAlgorithm": "CMAC",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/ivi5ksfsuplneuyt. Lo necesitará en el siguiente paso.

Crea el PVK

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_V2_VISA_PIN_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyMo
  --tags='[{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
                "Key": {
                    "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ov6icy4ryas4zcza",
```

```
                "KeyAttributes": {
                    "KeyUsage": "TR31_V2_VISA_PIN_VERIFICATION_KEY",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "TDES_2KEY",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": true,
                        "Sign": false,
                        "Verify": true,
                        "DeriveKey": false,
                        "NoRestrictions": false
                    }
                },
                "KeyCheckValue": "51A200",
                "KeyCheckValueAlgorithm": "ANSI_X9_24",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/ov6icy4ryas4zcza. Lo necesitará en el siguiente paso.

Genera un pin aleatorio, genera el PVV y devuelve el PIN y el PVV cifrados

Example

En este ejemplo, generaremos un nuevo pin (aleatorio) de 4 dígitos donde las salidas serán cifradas `PIN block` (. PinData PinBlock) y un `PVV` (PinData). VerificationValue). Las entradas clave son `PAN` el formato `Pin Verification Key` (también conocido como clave de generación de pines) `Pin Encryption Key` y el formato `PIN Block`.

Este comando requiere que la clave sea de tipo`TR31_V2_VISA_PIN_VERIFICATION_KEY`.

```
$ aws payment-cryptography-data generate-pin-data --generation-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2 --encryption-
```

```
key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/ivi5ksfsuplneuyt
 --primary-account-number 171234567890123 --pin-block-format ISO_FORMAT_0 --generation-
attributes VisaPin={PinVerificationKeyIndex=1}
```

```
{
            "GenerationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
            "GenerationKeyCheckValue": "7F2363",
            "EncryptionKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt",
            "EncryptionKeyCheckValue": "7CC9E2",
            "EncryptedPinBlock": "AC17DC148BDA645E",
            "PinData": {
                "VerificationValue": "5507"
            }
        }
```

Valide el PIN cifrado mediante el método PVV

Example

En este ejemplo, validaremos un PIN para un PAN determinado. Por lo general, el titular de la tarjeta o el usuario proporcionan el PIN durante el momento de la transacción para su validación y se compara con el valor registrado (la entrada del titular de la tarjeta se proporciona como un valor cifrado del terminal u otro proveedor principal). Para validar esta entrada, también se proporcionarán los siguientes valores en tiempo de ejecución: el pin cifrado, la clave utilizada para cifrar el pin de entrada (a menudo denominado IWK) PAN y el valor con el que realizar la verificación (a PVV o`PIN offset`).

Si la criptografía de AWS pago puede validar el PIN, se devuelve un http/200. Si el pin no está validado, devolverá un http/400.

```
$ aws payment-cryptography-data verify-pin-data --verification-key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/37y2tsl45p5zjbh2 --encryption-
key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/ivi5ksfsuplneuyt
 --primary-account-number 171234567890123 --pin-block-format ISO_FORMAT_0  --
verification-attributes VisaPin="{PinVerificationKeyIndex=1,VerificationValue=5507}" --
encrypted-pin-block AC17DC148BDA645E
```

```
{
```

```
        "VerificationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
        "VerificationKeyCheckValue": "7F2363",
        "EncryptionKeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
        "EncryptionKeyCheckValue": "7CC9E2",
}
```

Genera o verifica un CVV para una tarjeta determinada

CVV o CVV1 es un valor que tradicionalmente está incrustado en la banda magnética de una tarjeta. No es lo mismo que CVV2 (visible para el titular de la tarjeta y para su uso en compras en línea).

El primer paso es crear una clave. Para este tutorial, debe crear una clave CVK 3DES (2KEY TDES) de doble longitud.

> **Note**
>
> Tanto el CVV CVV2 como el iCVV utilizan algoritmos similares, si no idénticos, pero varían los datos de entrada. Todos utilizan el mismo tipo de clave TR31 _C0_CARD_VERIFICATION_KEY, pero se recomienda utilizar claves distintas para cada propósito. Se pueden distinguir mediante etiquetas de alias, como en el ejemplo siguiente. and/or

Crea la clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVV"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
r52o3wbqxyf6qlqr",
                "KeyAttributes": {
                    "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
```

```
                "KeyClass": "SYMMETRIC_KEY",
                "KeyAlgorithm": "TDES_2KEY",
                "KeyModesOfUse": {
                    "Encrypt": false,
                    "Decrypt": false,
                    "Wrap": false,
                    "Unwrap": false,
                    "Generate": true,
                    "Sign": false,
                    "Verify": true,
                    "DeriveKey": false,
                    "NoRestrictions": false
                }
            },
            "KeyCheckValue": "DE89F9",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
            "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/r52o3wbqxyf6qlqr. Lo necesitará en el siguiente paso.

Genera un CVV

Example

En este ejemplo, generaremos un CVV para un PAN determinado con entradas de 121PAN, un código de servicio (tal como se define en ISO/IEC 7813) y una fecha de caducidad de la tarjeta.

Para ver todos los parámetros disponibles, consulta el apartado CardVerificationValue1 de la guía de referencia de la API.

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
r52o3wbqxyf6qlqr --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue1='{CardExpiryDate=1127,ServiceCode=121}'
```

```
                {
                    "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/r52o3wbqxyf6qlqr",
                    "KeyCheckValue": "DE89F9",
                    "ValidationData": "801"
                }
```

Valide el CVV

Example

En este ejemplo, verificaremos el CVV de un PAN determinado introduciendo un CVK, un código de servicio 121PAN, la fecha de caducidad de la tarjeta y el CVV proporcionado durante la transacción para la validación.

Para ver todos los parámetros disponibles, consulte el apartado CardVerificationValue1 de la guía de referencia de la API.

> **Note**
>
> El CVV no es un valor introducido por el usuario (por ejemplo CVV2), sino que suele estar incrustado en una banda magnética. Se debe tener en cuenta si siempre debe validarse cuando se proporciona.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/r52o3wbqxyf6qlqr
 --primary-account-number=171234567890123 --verification-attributes
 CardVerificationValue1='{CardExpiryDate=1127,ServiceCode=121} --validation-data 801
```

```
{
                    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
r52o3wbqxyf6qlqr",
                    "KeyCheckValue": "DE89F9",
                    "ValidationData": "801"
}
```

Genera o verifica una CVV2 para una tarjeta específica

CVV2es un valor que tradicionalmente se indica en el reverso de una tarjeta y se utiliza para compras en línea. En el caso de las tarjetas virtuales, también puede mostrarse en una aplicación o en una pantalla. Criptográficamente, es igual CVV1 pero con un valor de código de servicio diferente.

Crea la clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVV2"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
               "Key": {
                   "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/7f7g4spf3xcklhzu",
                   "KeyAttributes": {
                       "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
                       "KeyClass": "SYMMETRIC_KEY",
                       "KeyAlgorithm": "TDES_2KEY",
                       "KeyModesOfUse": {
                           "Encrypt": false,
                           "Decrypt": false,
                           "Wrap": false,
                           "Unwrap": false,
                           "Generate": true,
                           "Sign": false,
                           "Verify": true,
                           "DeriveKey": false,
                           "NoRestrictions": false
                       }
                   },
                   "KeyCheckValue": "AEA5CD",
                   "KeyCheckValueAlgorithm": "ANSI_X9_24",
                   "Enabled": true,
                   "Exportable": true,
                   "KeyState": "CREATE_COMPLETE",
                   "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                   "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
```

```
                "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/7f7g4spf3xcklhzu. Lo necesitará en el siguiente paso.

Genera un CVV2

Example

En este ejemplo, generaremos un CVV2para un PAN determinado con entradas PAN y la fecha de caducidad de la tarjeta.

Para ver todos los parámetros disponibles, consulta el CardVerificationValueapartado 2 de la guía de referencia de la API.

```
$ aws payment-cryptography-data generate-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/7f7g4spf3xcklhzu
 --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue2='{CardExpiryDate=1127}'
```

```
                {
                    "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/7f7g4spf3xcklhzu",
                    "KeyCheckValue": "AEA5CD",
                    "ValidationData": "321"
                }
```

Valide un CVV2

Example

En este ejemplo, verificaremos a CVV2para un PAN determinado introduciendo un CVK, la fecha de caducidad de la tarjeta PAN y el CVV proporcionados durante la transacción para la validación.

Para ver todos los parámetros disponibles, consulte el apartado CardVerificationValue2 de la guía de referencia de la API.

> **Note**
>
> CVV2 y las demás entradas son valores introducidos por el usuario. Por lo tanto, no es necesariamente una señal de un problema que esto no se valide periódicamente.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/7f7g4spf3xcklhzu
 --primary-account-number=171234567890123 --verification-attributes
 CardVerificationValue2='{CardExpiryDate=1127} --validation-data 321
```

```
{
                      "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/7f7g4spf3xcklhzu",
                      "KeyCheckValue": "AEA5CD",
                      "ValidationData": "801"
   }
```

Genera o verifica un iCVV para una tarjeta específica

iCVV usa el mismo algoritmo que CVV/ CVV2 pero iCVV está integrado en una tarjeta con chip. Su código de servicio es 999.

Crea la clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"ICVV"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
               "Key": {
                   "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
c7dsi763r6s7lfp3",
                   "KeyAttributes": {
```

```
                    "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "TDES_2KEY",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": true,
                        "Sign": false,
                        "Verify": true,
                        "DeriveKey": false,
                        "NoRestrictions": false
                    }
                },
                "KeyCheckValue": "1201FB",
                "KeyCheckValueAlgorithm": "ANSI_X9_24",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/c7dsi763r6s7lfp3. Lo necesitará en el siguiente paso.

Genera un iCVV

Example

En este ejemplo, generaremos un iCVV para un PAN determinado con entradas dePAN, un código de servicio (tal como se define en ISO/IEC 7813) de 999 y una fecha de caducidad de la tarjeta.

Para ver todos los parámetros disponibles, consulta el apartado CardVerificationValue1 de la guía de referencia de la API.

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
c7dsi763r6s7lfp3 --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue1='{CardExpiryDate=1127,ServiceCode=999}'
```

```
                    {
                        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/c7dsi763r6s7lfp3",
                        "KeyCheckValue": "1201FB",
                        "ValidationData": "532"
                    }
```

Valide iCVV

Example

Para la validación, las entradas son el CVK, un código de servicio 999PAN, la fecha de caducidad de la tarjeta y el iCVV proporcionado durante la transacción para la validación.

Para ver todos los parámetros disponibles, consulte el apartado CardVerificationValue1 de la guía de referencia de la API.

> **Note**
>
> El iCVV no es un valor introducido por el usuario (por ejemplo CVV2), sino que suele estar incrustado en una EMV/chip tarjeta. Se debe tener en cuenta si siempre se debe validar cuando se proporciona.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/c7dsi763r6s7lfp3
 --primary-account-number=171234567890123 --verification-attributes
 CardVerificationValue1='{CardExpiryDate=1127,ServiceCode=999} --validation-data 532
```

```
{
                    "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/c7dsi763r6s7lfp3",
                    "KeyCheckValue": "1201FB",
                    "ValidationData": "532"
   }
```

Verifique un ARQC de EMV y genere un ARPC

El ARQC (criptograma de solicitud de autorización) es un criptograma generado por una tarjeta EMV (chip) y utilizado para validar los detalles de la transacción, así como el uso de una tarjeta autorizada. Incorpora datos de la tarjeta, el terminal y la propia transacción.

En el momento de la validación en el backend, se proporcionan las mismas entradas a AWS Payment Cryptography, el criptograma se recrea internamente y se compara con el valor proporcionado con la transacción. En este sentido, es similar a un MAC. El libro 2 de EMV 4.4 define tres aspectos de esta función: los métodos de derivación de claves (conocidos como clave de sesión común (CSK) para generar claves de transacción únicas, una carga útil mínima y los métodos para generar una respuesta (ARPC).

Los esquemas de tarjetas individuales pueden especificar campos transaccionales adicionales para incorporarlos o el orden en que aparecen esos campos. También existen otros esquemas de derivación específicos de esquemas (generalmente obsoletos) que se tratan en otra parte de esta documentación.

Para obtener más información, consulte la guía VerifyCardValidationDatade la API.

Crea la clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS,KeyClass=SYMMETRIC_KEY,KeyMod
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVN18"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
                "Key": {
                    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
                    "KeyAttributes": {
                        "KeyUsage": "TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS",
                        "KeyClass": "SYMMETRIC_KEY",
                        "KeyAlgorithm": "TDES_2KEY",
                        "KeyModesOfUse": {
                            "Encrypt": false,
                            "Decrypt": false,
```

```
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": false,
                        "Sign": false,
                        "Verify": false,
                        "DeriveKey": true,
                        "NoRestrictions": false
                    }
                },
                "KeyCheckValue": "08D7B4",
                "KeyCheckValueAlgorithm": "ANSI_X9_24",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/pw3s6nl62t5ushfk. Lo necesitará en el siguiente paso.

Genera un ARQC

El ARQC se genera exclusivamente mediante una tarjeta EMV. Por lo tanto, la criptografía AWS de pagos no tiene ninguna posibilidad de generar dicha carga útil. Con fines de prueba, hay varias bibliotecas disponibles en línea que pueden generar una carga útil adecuada, así como valores conocidos que generalmente proporcionan los distintos esquemas.

Valide un ARQC

Example

Si la criptografía de AWS pagos puede validar el ARQC, se devuelve un http/200. Opcionalmente, se puede proporcionar un ARPC (respuesta) e incluirlo en la respuesta una vez validado el ARQC.

```
$ aws payment-cryptography-data verify-auth-request-cryptogram
 --auth-request-cryptogram 61EDCC708B4C97B4 --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk
 --major-key-derivation-mode EMV_OPTION_A --transaction-data
 00000000170000000000000008400080008000084016051700000000093800000B1F220103000000000000000000000
```

```
 --session-key-derivation-attributes='{"EmvCommon":
{"ApplicationTransactionCounter":"000B",
 "PanSequenceNumber":"01","PrimaryAccountNumber":"9137631040001422"}}' --auth-response-
attributes='{"ArpcMethod2":{"CardStatusUpdate":"12345678"}}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
    "KeyCheckValue": "08D7B4",
    "AuthResponseValue":"2263AC85"
}
```

Genere y verifique un MAC EMV

EMV MAC es un MAC que utiliza la entrada de una clave derivada de EMV y, a continuación, realiza un MAC ISO9797 -3 (minorista) sobre los datos resultantes. El EMV MAC se utiliza normalmente para enviar comandos a una tarjeta EMV, por ejemplo, para desbloquear scripts.

> **Note**
>
> AWS La criptografía de pagos no valida el contenido del script. Consulte el manual de su esquema o tarjeta para obtener detalles sobre los comandos específicos que debe incluir.

Para obtener más información, consulta MacAlgorithmEmvla guía de la API.

Temas

- Crea la clave
- Genere un EMV MAC

Crea la clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E2_EMV_MKEY_INTEGRITY,KeyClass=SYMMETRIC_KEY,KeyModesOfUs
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVN18"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
        "Key": {
            "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
            "KeyAttributes": {
                "KeyUsage": "TR31_E2_EMV_MKEY_INTEGRITY",
                "KeyClass": "SYMMETRIC_KEY",
                "KeyAlgorithm": "TDES_2KEY",
                "KeyModesOfUse": {
                    "Encrypt": false,
                    "Decrypt": false,
                    "Wrap": false,
                    "Unwrap": false,
                    "Generate": false,
                    "Sign": false,
                    "Verify": false,
                    "DeriveKey": true,
                    "NoRestrictions": false
                }
            },
            "KeyCheckValue": "08D7B4",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
            "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
        }
    }
```


Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/pw3s6nl62t5ushfk. Lo necesitará en el siguiente paso.

Genere un EMV MAC

Lo habitual es que un proceso interno genere un script EMV (por ejemplo, para desbloquear una tarjeta), lo firme con este comando (que obtiene una clave de un solo uso específica para una tarjeta en particular) y, a continuación, devuelva el MAC. A continuación, se envía el comando + MAC a la tarjeta que se va a aplicar. Enviar el comando a la tarjeta está fuera del ámbito de la criptografía de AWS pagos.

> **Note**
>
> Este comando está diseñado para comandos en los que no se envían datos cifrados (como el PIN). EMV Encrypt se puede combinar con este comando para añadir datos cifrados al script del emisor antes de ejecutar este comando

Datos del mensaje

Los datos del mensaje incluyen el encabezado y el comando de la APDU. Si bien esto puede variar según la implementación, en este ejemplo se utiliza el encabezado APDU para desbloquear (84 24 00 00 08), seguido del ATC (0007) y, por último, del ARQC de la transacción anterior (999E57 F47CACE). FD0 El servicio no valida el contenido de este campo.

Modo de derivación de claves de sesión

Este campo define cómo se genera la clave de sesión. Por lo general, EMV_COMMON_SESSION_KEY se usa para las nuevas implementaciones, mientras que EMV2000 | AMEX | MASTERCARD_SESSION_KEY | VISA también se puede usar.

MajorKeyDerivationMode

EMV define el modo A, B o C. El modo A es el más común y la criptografía de pagos actualmente admite el modo A o el modo B. AWS

PAN

El número de cuenta, normalmente disponible en el campo de chip 5A o en ISO8583 el campo 2, pero también se puede recuperar del sistema de tarjetas.

PSN

El número de secuencia de la tarjeta. Si no se utiliza, introduzca 00.

SessionKeyDerivationValue

Estos son los datos de derivación por sesión. Puede ser el último ARQC (ApplicationCryptogram) del campo 9F26 o el último ATC del 9F36, según el esquema de derivación.

Rellenado

El relleno se aplica automáticamente y utiliza el método 2 de relleno 9797-1. ISO/IEC

Example

```
$ aws payment-cryptography-data generate-mac --message-data
 842400000800079 99E57FD0F47CACE --key-identifier arn:aws:payment-
cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk --message-
data 8424000008999E57FD0F47CACE0007 --generation-attributes
 EmvMac="{MajorKeyDerivationMode=EMV_OPTION_A,PanSequenceNumber='00',PrimaryAccountNumber='2235
```

```
{
"KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk",
"KeyCheckValue": "08D7B4",
"Mac":"5652EEDF83EA0D84"
}
```

Genera un EMV MAC para el cambio de PIN

El cambio de PIN EMV combina dos operaciones: generar un MAC para un script del emisor y cifrar un nuevo PIN para cambiarlo sin conexión a Internet en una tarjeta con chip EMV. Este comando solo es necesario en algunos países en los que el PIN está almacenado en la tarjeta con chip (esto es habitual en los países europeos). Suele utilizarse cuando el titular de la tarjeta necesita cambiar su PIN y el nuevo PIN debe transmitirse de forma segura a la tarjeta junto con un MAC para comprobar la autenticidad del comando.

> **Note**
>
> Si solo necesitas enviar comandos a la tarjeta pero no cambiar el PIN, considera usar los comandos ARPC CSU o Generate EMV MAC en su lugar.

Para obtener más información, consulte la guía de GenerateMacEmvPinChangela API.

Genera un EMV (MAC) y un PIN cifrado para cambiarlo.

Esta operación requiere dos claves: una clave de integridad EMV (: TR31 _E2_EMV_MKEY_INTEGRITY) para la generación del MAC y una clave de confidencialidad EMV (KeyUsage: _E4_EMV_MKEY_CONFIDENCIALITY) para el cifrado del PIN. KeyUsage TR31 Lo habitual es que un proceso interno genere un script de cambio de PIN EMV, que incluye tanto el MAC del script del emisor como el PIN nuevo cifrado. A continuación, el comando y el PIN cifrado se envían a la tarjeta para actualizar el PIN sin conexión. Enviar el comando a la tarjeta está fuera del ámbito de la criptografía de AWS pagos.

Datos del mensaje

Los datos del mensaje incluyen el comando APDU para el script del emisor. El servicio no valida el contenido de este campo.

Nuevo bloque de PIN cifrado

El nuevo bloque de PIN cifrado que se enviará a la tarjeta. Debe proporcionarse como un valor cifrado mediante una clave de cifrado PIN.

Nuevo identificador PIN PEK

La clave utilizada para cifrar el nuevo PIN antes de pasarlo a esta API.

Clave de integridad de mensajería segura

La clave de integridad EMV (KeyUsage: TR31 _E2_EMV_MKEY_INTEGRITY) utilizada para la generación de MAC.

Clave de confidencialidad de mensajería segura

La clave de confidencialidad EMV (KeyUsage: TR31 _E4_EMV_MKEY_CONFIDENCIALITY) utilizada para el cifrado con PIN.

MajorKeyDerivationMode

EMV define el modo A, B o C. El modo A es el más común y la criptografía de pagos actualmente admite el modo A o el modo B. AWS

Mode

El modo de cifrado, normalmente CBC para las operaciones de cambio de PIN.

PAN

El número de cuenta, normalmente disponible en el campo 5A o ISO8583 2 con chip, pero también se puede recuperar del sistema de tarjetas.

PanSequenceNumber

El número de secuencia de la tarjeta. Si no se utiliza, introduzca 00.

ApplicationCryptogram

Estos son los datos de derivación por sesión, normalmente el último ARQC del campo 9F26.

PinBlockLengthPosition

Especifica dónde está codificada la longitud del bloque de PIN. Normalmente se establece en NINGUNO. Comprueba las especificaciones de tu esquema de tarjetas si no estás seguro.

PinBlockPaddingType

Especifica el tipo de relleno del bloque de PIN. Normalmente se establece en NO_PADDING. Comprueba las especificaciones del esquema de tu tarjeta si no estás seguro.

Example

```
$ aws payment-cryptography-data generate-mac-emv-pin-change \
    --message-data 00A4040008A000000004101080D8050000000101 0A04000000000000 \
    --new-encrypted-pin-block 67FB27C75580EFE7 \
    --new-pin-pek-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt \
    --pin-block-format ISO_FORMAT_0 \
    --secure-messaging-confidentiality-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/tqv5yij6wtxx64pi \
    --secure-messaging-integrity-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/pw3s6nl62t5ushfk \
    --derivation-method-attributes
 'EmvCommon={ApplicationCryptogram=1234567890123457,MajorKeyDerivationMode=EMV_OPTION_A,Mode=CB
```

```
{
    "SecureMessagingIntegrityKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/pw3s6nl62t5ushfk",
    "SecureMessagingIntegrityKeyCheckValue": "08D7B4",
    "SecureMessagingConfidentialityKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/tqv5yij6wtxx64pi",
    "SecureMessagingConfidentialityKeyCheckValue": "C1EB8F",
    "Mac": "5652EEDF83EA0D84",
    "EncryptedPinBlock": "F1A2B3C4D5E6F7A8"
}
```

Funciones específicas de la red

Temas

- Funciones específicas de visa
- Funciones específicas de Mastercard

- Funciones específicas de American Express
- Funciones específicas de JCB

Funciones específicas de visa

Temas

- ARQC -/ CVN18CVN22
- ARQC - CVN10
- 3D CAVV V7
- dCVV (valor de verificación dinámica de la tarjeta) - CVN17

ARQC -/ CVN18CVN22

CVN18 y CVN22 utilice el método CSK de derivación de claves. Los datos exactos de las transacciones varían entre estos dos métodos. Consulte la documentación del esquema para obtener más información sobre cómo crear el campo de datos de transacciones.

ARQC - CVN10

CVN10 es un método más antiguo de Visa para las transacciones EMV que utiliza la obtención de la clave por tarjeta en lugar de la derivación de la sesión (por transacción) y también utiliza una carga útil diferente. Para obtener información sobre el contenido de la carga útil, ponte en contacto con el programa para obtener más información.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS,KeyClass=SYMMETRIC_KEY,KeyMod
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVN10"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
                "KeyAttributes": {
```

```
                "KeyUsage": "TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS",
                "KeyClass": "SYMMETRIC_KEY",
                "KeyAlgorithm": "TDES_2KEY",
                "KeyModesOfUse": {
                    "Encrypt": false,
                    "Decrypt": false,
                    "Wrap": false,
                    "Unwrap": false,
                    "Generate": false,
                    "Sign": false,
                    "Verify": false,
                    "DeriveKey": true,
                    "NoRestrictions": false
                }
            },
            "KeyCheckValue": "08D7B4",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
            "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/pw3s6nl62t5ushfk. Lo necesitará en el siguiente paso.

Valide el ARQC

Example

En este ejemplo, validaremos un ARQC generado con Visa. CVN10

Si la criptografía de AWS pagos puede validar el ARQC, se devuelve un http/200. Si el arqc no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-auth-request-cryptogram --auth-request-
cryptogram D791093C8A921769 \
  --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk \
  --major-key-derivation-mode EMV_OPTION_A \
```

```
  --transaction-data
 0000000017000000000000000840008000800008401605170000000009380000B03011203000000 \
  --session-key-derivation-attributes='{"Visa":{"PanSequenceNumber":"01" \
  ,"PrimaryAccountNumber":"9137631040001422"}}'
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
    "KeyCheckValue": "08D7B4"
  }
```

3D CAVV V7

En el caso de las transacciones con Visa Secure (3DS), el servidor de control de acceso (ACS) del emisor genera un CAVV (valor de verificación de autenticación del titular de la tarjeta). El CAVV es una prueba de que se ha realizado la autenticación del titular de la tarjeta, es único para cada transacción de autenticación y lo proporciona el adquirente en el mensaje de autorización. La versión 7 del CAVV vincula a la aprobación los datos adicionales sobre la transacción, incluidos elementos como el nombre del vendedor, el importe de la compra y la fecha de compra. De esta forma, se trata, en efecto, de un hash criptográfico de la carga útil de la transacción.

Criptográficamente, el CAVV V7 utiliza el algoritmo CVV, pero todas las entradas han sido changed/ repurposed. Please consult appropriate third party/Visa documentación sobre cómo producir las entradas para generar una carga útil del CAVV V7.

Crea la clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"CAVV-V7"},
{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
dnaeyrjgdjjtw6dk",
                "KeyAttributes": {
```

```
                "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
                "KeyClass": "SYMMETRIC_KEY",
                "KeyAlgorithm": "TDES_2KEY",
                "KeyModesOfUse": {
                    "Encrypt": false,
                    "Decrypt": false,
                    "Wrap": false,
                    "Unwrap": false,
                    "Generate": true,
                    "Sign": false,
                    "Verify": true,
                    "DeriveKey": false,
                    "NoRestrictions": false
                }
            },
            "KeyCheckValue": "F3FB13",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
            "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/dnaeyrjgdjjtw6dk. Lo necesitará en el siguiente paso.

Genera un CAVV V7

Example

En este ejemplo, generaremos un CAVV V7 para una transacción determinada con las entradas especificadas en las especificaciones. Tenga en cuenta que, en el caso de este algoritmo, los campos se pueden reutilizar o reutilizar, por lo que no se debe suponer que las etiquetas de los campos coinciden con las entradas.

Para ver todos los parámetros disponibles, consulte el apartado CardVerificationValue1 de la guía de referencia de la API.

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
```

```
dnaeyrjgdjjtw6dk --primary-account-number=171234567890123 --generation-attributes
 CardVerificationValue1='{CardExpiryDate=9431,ServiceCode=431}'
```

```
            {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
dnaeyrjgdjjtw6dk",
                "KeyCheckValue": "F3FB13",
                "ValidationData": "491"
            }
```

Valide el CAVV V7

Example

Para la validación, las entradas son el CVK, los valores de entrada calculados y el CAVV proporcionados durante la transacción para la validación.

Para ver todos los parámetros disponibles, consulte el apartado CardVerificationValue1 de la guía de referencia de la API.

> **Note**
>
> El CAVV no es un valor introducido por el usuario (por ejemplo CVV2), sino que lo calcula el emisor ACS. Se debe tener en cuenta si siempre debe validarse cuando se proporciona.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/dnaeyrjgdjjtw6dk
 --primary-account-number=171234567890123 --verification-attributes
 CardVerificationValue1='{CardExpiryDate=9431,ServiceCode=431} --validation-data 491
```

```
{
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
dnaeyrjgdjjtw6dk",
                "KeyCheckValue": "F3FB13",
                "ValidationData": "491"
```

```
}
```

dCVV (valor de verificación dinámica de la tarjeta) - CVN17

El dCVV (valor dinámico de verificación de la tarjeta) es un criptograma dinámico específico para visados que se utiliza para las transacciones EMV sin contacto. Se lo conoce como EMV primitivo y proporciona una mayor seguridad al generar un valor de verificación único para cada transacción. El dCVV utiliza entradas como el número de cuenta principal (PAN), el número de secuencia PAN (PSN), el contador de transacciones de aplicaciones (ATC), el número impredecible y los datos de seguimiento. Todavía se usa en algunos lugares, pero ha sido reemplazado en su mayoría por otros algoritmos similares. CVN18

Para ver todos los parámetros disponibles, consulta DynamicCardVerificationValuela guía de referencia de la API.

Crea una clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E4_EMV_MKEY_DYNAMIC_NUMBERS,KeyClass=SYMMETRIC_KEY,KeyMod
 --tags='[{"Key":"KEY_PURPOSE","Value":"DCVV"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
mw7dn3qxvkfh8ztc",
                "KeyAttributes": {
                    "KeyUsage": "TR31_E4_EMV_MKEY_DYNAMIC_NUMBERS",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "TDES_2KEY",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": true,
                        "Sign": false,
                        "Verify": true,
                        "DeriveKey": false,
```

```
                    "NoRestrictions": false
                }
            },
            "KeyCheckValue": "A8E4D2",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2025-02-02T11:45:30.648000-08:00",
            "UsageStartTimestamp": "2025-02-02T11:45:30.626000-08:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/mw7dn3qxvkfh8ztc. Lo necesitará en el siguiente paso.

Genera un dCVv

Example

En este ejemplo, generaremos un dCVV para una transacción EMV sin contacto. Las entradas incluyen el PAN, el número de secuencia PAN, el contador de transacciones de la aplicación, el número impredecible y los datos de seguimiento.

```
$ aws payment-cryptography-data generate-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/mw7dn3qxvkfh8ztc \
    --primary-account-number=5111112627662122 \
    --generation-attributes
 DynamicCardVerificationValue='{ApplicationTransactionCounter=01,PanSequenceNumber=00,TrackData
 \
    --validation-data-length 5
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
mw7dn3qxvkfh8ztc",
    "KeyCheckValue": "A8E4D2",
    "ValidationData": "36667"
}
```

Valide el dCVV

Example

En este ejemplo, validaremos un dCVV proporcionado durante una transacción. Para la validación, se deben proporcionar las mismas entradas utilizadas para la generación.

Si la criptografía de AWS pagos puede validarse, se devuelve un http/200. Si el valor no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/mw7dn3qxvkfh8ztc \
    --primary-account-number=5111112627662122 \
    --validation-data=36667 \
    --verification-attributes
 DynamicCardVerificationValue='{ApplicationTransactionCounter=01,PanSequenceNumber=00,TrackData
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
mw7dn3qxvkfh8ztc",
    "KeyCheckValue": "A8E4D2"
}
```

Funciones específicas de Mastercard

Temas

- DCVC3
- ARQC -/ CVN14CVN15
- ARQC -/ CVN12CVN13
- SPA2 3DS AAV

DCVC3

DCVC3 es anterior a los CVN12 esquemas EMV, CSK y Mastercard y representa otro enfoque para utilizar claves dinámicas. A veces también se reutiliza para otros casos de uso. En este esquema, las entradas son datos PAN, PSN, Track1/Track2, un contador impredecible de números y transacciones (ATC).

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E4_EMV_MKEY_DYNAMIC_NUMBERS,KeyClass=SYMMETRIC_KEY,KeyMod
 --tags='[{"Key":"KEY_PURPOSE","Value":"DCVC3"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
hrh6qgbi3sk4y3wq",
                "KeyAttributes": {
                    "KeyUsage": "TR31_E4_EMV_MKEY_DYNAMIC_NUMBERS",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "TDES_2KEY",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": false,
                        "Sign": false,
                        "Verify": false,
                        "DeriveKey": true,
                        "NoRestrictions": false
                    }
                },
                "KeyCheckValue": "08D7B4",
                "KeyCheckValueAlgorithm": "ANSI_X9_24",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/hrh6qgbi3sk4y3wq. Lo necesitará en el siguiente paso.

Genera un DCVC3

Example

Aunque normalmente DCVC3 se genera mediante una tarjeta con chip, también se puede generar manualmente, como en este ejemplo

```
$ aws payment-cryptography-data generate-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk
 --primary-account-number=5413123456784808 --generation-attributes
 DynamicCardVerificationCode='{ApplicationTransactionCounter=0000,TrackData=524106000000069D13
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
    "KeyCheckValue": "08D7B4",
    "ValidationData": "865"
  }
```

Valide el DCVC3

Example

En este ejemplo, validaremos un DCVC3. Tenga en cuenta que el ATC debe proporcionarse como un número hexadecimal, por ejemplo, un contador de 11 debe representarse como 000B. El servicio espera un valor de 3 dígitos DCVC3, por lo que si ha almacenado un valor de 4 (o 5) dígitos, simplemente trunque los caracteres de la izquierda hasta que tenga 3 dígitos (por ejemplo, 15321 debería dar como resultado un valor de 321 para los datos de validación).

Si la criptografía AWS de pagos puede validarse, se devolverá un http/200. Si el valor no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-card-validation-data  --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/pw3s6nl62t5ushfk
 --primary-account-number=5413123456784808 --verification-attributes
 DynamicCardVerificationCode='{ApplicationTransactionCounter=000B,TrackData=524106000000069D13
 --validation-data 398
```

```
{
```

```
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
    "KeyCheckValue": "08D7B4"
  }
```

ARQC -/ CVN14CVN15

CVN14 y CVN15 utilice el método EMV CSK de derivación de claves. Los datos exactos de las transacciones varían entre estos dos métodos; consulte la documentación del esquema para obtener más información sobre cómo crear el campo de datos de transacciones.

ARQC -/ CVN12CVN13

CVN12 y CVN13 son un método antiguo específico de MasterCard para transacciones EMV que incorpora un número impredecible en la derivación por transacción y también utiliza una carga útil diferente. Para obtener información sobre el contenido de la carga útil, póngase en contacto con el programa.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS,KeyClass=SYMMETRIC_KEY,KeyMod
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVN12"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
                "KeyAttributes": {
                    "KeyUsage": "TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "TDES_2KEY",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": false,
                        "Sign": false,
```

```
                    "Verify": false,
                    "DeriveKey": true,
                    "NoRestrictions": false
                }
            },
            "KeyCheckValue": "08D7B4",
            "KeyCheckValueAlgorithm": "ANSI_X9_24",
            "Enabled": true,
            "Exportable": true,
            "KeyState": "CREATE_COMPLETE",
            "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
            "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
            "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/pw3s6nl62t5ushfk. Lo necesitará en el siguiente paso.

Valide el ARQC

Example

En este ejemplo, validaremos un ARQC generado con Mastercard. CVN12

Si la criptografía de AWS pagos puede validar el ARQC, se devuelve un http/200. Si el arqc no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-auth-request-cryptogram --auth-request-
cryptogram 31BE5D49F14A5F01 \
  --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk \
  --major-key-derivation-mode EMV_OPTION_A \
  --transaction-data
 00000000170000000000000008400080008000084016051700000000093800000B1F220103000000000000000000000
 \
  --session-key-derivation-attributes='{"MastercardSessionKey":
{"ApplicationTransactionCounter":"000B","PanSequenceNumber":"01","PrimaryAccountNumber":"541312
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
```

```
    "KeyCheckValue": "08D7B4"
  }
```

SPA2 3DS AAV

SPA2(Aplicación de pago seguro) El AAV (valor de autenticación de la cuenta) se utiliza para las transacciones 3DS con Mastercard (también conocidas como Mastercard Idenity Check). Proporciona autenticación criptográfica para las transacciones de comercio electrónico mediante la generación de MAC basada en HMAC. El AAV se genera utilizando datos específicos de la transacción y una clave secreta compartida.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=HMAC_SHA256,KeyUsage=TR31_M7_HMAC_KEY,KeyClass=SYMMETRIC_KEY,KeyModesOfUse='{Gene
 --tags='[{"Key":"KEY_PURPOSE","Value":"SPA2_AAV"},
{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-west-2:111122223333:key/
q5vjtshsg67cz5gn",
                "KeyAttributes": {
                    "KeyUsage": "TR31_M7_HMAC_KEY",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "HMAC_SHA256",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": true,
                        "Sign": false,
                        "Verify": true,
                        "DeriveKey": false,
                        "NoRestrictions": false
                    }
                },
```

```
                "KeyCheckValue": "C661F9",
                "KeyCheckValueAlgorithm": "HMAC",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-west- 2:111122223333:key/q5vjtshsg67cz5gn. Lo necesitará en el siguiente paso.

Genera AAV SPA2

Example

En este ejemplo, generaremos el componente del valor de autenticación del emisor (IAV) del AAV mediante la generación de SPA2 HMAC MAC. Los datos del mensaje contienen la información específica de la transacción que se autenticará. El formato de los datos del mensaje debe seguir las SPA2 especificaciones de Mastercard y no se describe en este ejemplo.

> **Note**
>
> Revise las especificaciones de formato de su tarjeta Mastercard para insertar el IAV en el valor del AAV.

```
$ aws payment-cryptography-data generate-mac --key-identifier arn:aws:payment-
cryptography:us-west-2:111122223333:key/q5vjtshsg67cz5gn --message-data
 "2226400099919520FFFFd8b448be65694fe7b42f836bad396e9d" --generation-attributes
 Algorithm=HMAC --region us-west-2
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-west-2:111122223333:key/
q5vjtshsg67cz5gn",
    "KeyCheckValue": "C661F9",
    "Mac": "6FB2405E9D8A4C1F7B173F73ADD1A6DC358531CAB0E9994FC5B62012ADDE91FC"
}
```

Verifica el AAV SPA2

Example

En este ejemplo, verificaremos un SPA2 AAV. Para la verificación, se proporcionan los mismos datos del mensaje y el mismo valor MAC.

Si la criptografía de AWS pago puede validar el MAC, se devuelve un http/200. Si el MAC no está validado, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-mac --key-identifier arn:aws:payment-
cryptography:us-west-2:111122223333:key/q5vjtshsg67cz5gn --message-
data "2226400099919520FFFFd8b448be65694fe7b42f836bad396e9d" --mac
 "6FB2405E9D8A4C1F7B173F73ADD1A6DC358531CAB0E9994FC5B62012ADDE91FC" --verification-
attributes Algorithm=HMAC --region us-west-2
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-west-2:111122223333:key/
q5vjtshsg67cz5gn",
    "KeyCheckValue": "C661F9"
}
```

Funciones específicas de American Express

Temas

- CSC1
- CSC2
- iCSC
- 3D AEVV

CSC1

La versión 1 de CSC también se conoce como algoritmo CSC clásico. El servicio puede proporcionarlo como un número de 3,4 o 5 dígitos.

Para ver todos los parámetros disponibles, consulte el AmexCardSecurityCodeVersionpunto 1 en la guía de referencia de la API.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"CSC1"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
                "Key": {
                    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
esh6hn7pxdtttzgq",
                    "KeyAttributes": {
                        "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
                        "KeyClass": "SYMMETRIC_KEY",
                        "KeyAlgorithm": "TDES_2KEY",
                        "KeyModesOfUse": {
                            "Encrypt": false,
                            "Decrypt": false,
                            "Wrap": false,
                            "Unwrap": false,
                            "Generate": true,
                            "Sign": false,
                            "Verify": true,
                            "DeriveKey": false,
                            "NoRestrictions": false
                        }
                    },
                    "KeyCheckValue": "8B5077",
                    "KeyCheckValueAlgorithm": "ANSI_X9_24",
                    "Enabled": true,
                    "Exportable": true,
                    "KeyState": "CREATE_COMPLETE",
                    "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                    "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
                    "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
                }
            }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/esh6hn7pxdtttzgq. Lo necesitará en el siguiente paso.

Genera un CSC1

Example

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
esh6hn7pxdtttzgq --primary-account-number=344131234567848 --generation-attributes
 AmexCardSecurityCodeVersion1='{CardExpiryDate=1224}' --validation-data-length 4
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
esh6hn7pxdtttzgq",
    "KeyCheckValue": "8B5077",
    "ValidationData": "3938"
  }
```

Valide el CSC1

Example

En este ejemplo, validaremos un CSC1.

Si la criptografía de AWS pago puede validarse, se devuelve un http/200. Si el valor no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-card-validation-data  --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/esh6hn7pxdtttzgq
 --primary-account-number=344131234567848 --verification-attributes
 AmexCardSecurityCodeVersion1='{CardExpiryDate=1224}''  --validation-data 3938
```

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
esh6hn7pxdtttzgq",
    "KeyCheckValue": "8B5077"
  }
```

CSC2

La versión 2 del CSC también se conoce como algoritmo CSC mejorado. El servicio puede proporcionarlo como un número de 3,4 o 5 dígitos. El código de servicio CSC2 suele ser 000.

Para ver todos los parámetros disponibles, consulte el AmexCardSecurityCodeVersionapartado 2 en la guía de referencia de la API.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"CSC2"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
            "Key": {
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
erlm445qvunmvoda",
                "KeyAttributes": {
                    "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY",
                    "KeyClass": "SYMMETRIC_KEY",
                    "KeyAlgorithm": "TDES_2KEY",
                    "KeyModesOfUse": {
                        "Encrypt": false,
                        "Decrypt": false,
                        "Wrap": false,
                        "Unwrap": false,
                        "Generate": true,
                        "Sign": false,
                        "Verify": true,
                        "DeriveKey": false,
                        "NoRestrictions": false
                    }
                },
                "KeyCheckValue": "BF1077",
                "KeyCheckValueAlgorithm": "ANSI_X9_24",
                "Enabled": true,
                "Exportable": true,
                "KeyState": "CREATE_COMPLETE",
                "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                "CreateTimestamp": "2023-06-05T06:41:46.648000-07:00",
                "UsageStartTimestamp": "2023-06-05T06:41:46.626000-07:00"
            }
        }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/erlm445qvunmvoda. Lo necesitará en el siguiente paso.

Genera un CSC2

En este ejemplo, generaremos a CSC2 con una longitud de 4. El CSC se puede generar con una longitud de 3,4 o 5. Para American Express, PANs debe tener 15 dígitos y empezar por 34 o 37. La fecha de caducidad suele tener el formato YYMM. El código de servicio puede variar; consulte el manual, pero los valores típicos son 000, 201 o 702

Example

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
erlm445qvunmvoda --primary-account-number=344131234567848 --generation-attributes
 AmexCardSecurityCodeVersion2='{CardExpiryDate=2412,ServiceCode=000}' --validation-
data-length 4
```

```
{
"KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/erlm445qvunmvoda",
"KeyCheckValue": "BF1077",
"ValidationData": "3982"
}
```

Valide el CSC2

Example

En este ejemplo, validaremos un CSC2.

Si la criptografía de AWS pago puede validarse, se devuelve un http/200. Si el valor no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-card-validation-data  --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/erlm445qvunmvoda
 --primary-account-number=344131234567848 --verification-attributes
 AmexCardSecurityCodeVersion2='{CardExpiryDate=2412,ServiceCode=000}' --validation-data
 3982
```

```
{
```

```
"KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/erlm445qvunmvoda",
"KeyCheckValue": "BF1077"
}
```

iCSC

El iCSC también se conoce como algoritmo CSC estático y se calcula con la versión 2 del CSC. El servicio puede proporcionarlo como un número de 3,4 o 5 dígitos.

Use el código de servicio 999 para calcular el iCSC de una tarjeta de contacto. Utilice el código de servicio 702 para calcular el iCSC de una tarjeta sin contacto.

Para ver todos los parámetros disponibles, consulte el apartado AmexCardSecurityCodeVersion2 de la guía de referencia de la API.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"CSC1"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
        "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-
east-1:111122223333:key/7vrybrbvjcvwtunv",
        "KeyAttributes": {
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
```

```
            },
        },
        "KeyCheckValue": "7121C7",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "Enabled": true,
        "Exportable": true,
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "CreateTimestamp": "2025-01-29T09:19:21.209000-05:00",
        "UsageStartTimestamp": "2025-01-29T09:19:21.192000-05:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 1:111122223333:key/7vrybrbvjcvwtunv. Lo necesitará en el siguiente paso.

Genera un iCSC

En este ejemplo, generaremos un iCSC con una longitud de 4 para una tarjeta sin contacto utilizando el código de servicio 702. El CSC se puede generar con una longitud de 3,4 o 5. Para American Express, PANs debe tener 15 dígitos y empezar por 34 o 37.

Example

```
$ aws payment-cryptography-data generate-card-validation-data --key-identifier
 arn:aws:payment-cryptography:us-east-1:111122223333:key/7vrybrbvjcvwtunv
 --primary-account-number=344131234567848 --generation-attributes
 AmexCardSecurityCodeVersion2='{CardExpiryDate=1224,ServiceCode=702}' --validation-
data-length 4
```

```
{
    "KeyArn": arn:aws:payment-cryptography:us-east-1:111122223333:key/7vrybrbvjcvwtunv,
    "KeyCheckValue": 7121C7,
    "ValidationData": "2365"
}
```

Valide el iCSC

Example

En este ejemplo, validaremos un iCSC.

Si la criptografía de AWS pago puede validarse, se devuelve un http/200. Si el valor no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-card-validation-data  --key-identifier
 arn:aws:payment-cryptography:us-east-1:111122223333:key/7vrybrbvjcvwtunv
 --primary-account-number=344131234567848 --verification-attributes
 AmexCardSecurityCodeVersion2='{CardExpiryDate=1224,ServiceCode=702}' --validation-data
 2365
```

```
{
    "KeyArn": arn:aws:payment-cryptography:us-east-1:111122223333:key/7vrybrbvjcvwtunv,
    "KeyCheckValue": 7121C7
}
```

3D AEVV

El AEVV (valor de verificación de la cuenta 3-D Secure) de 3DS se utiliza para la autenticación 3-D Secure de American Express. Utiliza el mismo algoritmo CSC2 pero con parámetros de entrada diferentes. El campo de fecha de caducidad debe rellenarse con un número impredecible (aleatorio) y el código de servicio consta del código de resultados de la autenticación AEVV (1 dígito) más el código de autenticación de segundo factor (2 dígitos). La longitud de salida debe ser de 3 dígitos.

Para ver todos los parámetros disponibles, consulte el AmexCardSecurityCodeVersionapartado 2 de la guía de referencia de la API.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC_KEY,KeyModesO
 --tags='[{"Key":"KEY_PURPOSE","Value":"3DS_AEVV"},
{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
        "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kw8djn5qxvfh3ztm",
        "KeyAttributes": {
```

```
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
        },
        "KeyCheckValue": "8F3A21",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "Enabled": true,
        "Exportable": true,
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "CreateTimestamp": "2025-02-02T10:30:15.209000-05:00",
        "UsageStartTimestamp": "2025-02-02T10:30:15.192000-05:00"
        }
    }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/kw8djn5qxvfh3ztm. Lo necesitará en el siguiente paso.

Genera un AEVV para 3DS

En este ejemplo, generaremos un AEVV de 3DS con una longitud de 3. El campo de fecha de caducidad contiene un número impredecible (aleatorio) (por ejemplo, 1234) y el código de servicio consta del código de resultados de autenticación AEVV (1 dígito) más el código de autenticación de segundo factor (2 dígitos), por ejemplo, 543, donde 5 es el código de resultados de autenticación y 43 es el código de autenticación de segundo factor. En el caso de American Express, PANs debe tener 15 dígitos y empezar por 34 o 37.

Example

```
$ aws payment-cryptography-data generate-card-validation-data --key-
identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
```

```
kw8djn5qxvfh3ztm --primary-account-number=344131234567848 --generation-attributes
 AmexCardSecurityCodeVersion2='{CardExpiryDate=1234,ServiceCode=543}' --validation-
data-length 3
```

```
{
    "KeyArn": arn:aws:payment-cryptography:us-east-2:111122223333:key/kw8djn5qxvfh3ztm,
    "KeyCheckValue": 8F3A21,
    "ValidationData": "921"
}
```

Valide el AEVV de la 3DS

Example

En este ejemplo, validaremos un AEVV de la 3DS.

Si la criptografía de AWS pago puede validarse, se devuelve un http/200. Si el valor no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-card-validation-data  --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/kw8djn5qxvfh3ztm
 --primary-account-number=344131234567848 --verification-attributes
 AmexCardSecurityCodeVersion2='{CardExpiryDate=1234,ServiceCode=543}' --validation-data
 921
```

```
{
    "KeyArn": arn:aws:payment-cryptography:us-east-2:111122223333:key/kw8djn5qxvfh3ztm,
    "KeyCheckValue": 8F3A21
}
```

Funciones específicas de JCB

Temas

- ARQC - CVN04
- ARQC - CVN01

ARQC - CVN04

JCB CVN04 utiliza el método CSK de derivación de claves. Consulte la documentación del esquema para obtener detalles sobre cómo crear el campo de datos de transacciones.

ARQC - CVN01

CVN01 es un método más antiguo de JCB para transacciones EMV que utiliza la derivación por clave de tarjeta en lugar de la derivación por sesión (por transacción) y también utiliza una carga útil diferente. Visa también usa este mensaje, por lo que el nombre del elemento lleva ese nombre, aunque también se usa para JCB. Para obtener información sobre el contenido de la carga útil, póngase en contacto con la documentación del programa.

Crear clave

```
$ aws payment-cryptography create-key --exportable --key-attributes
 KeyAlgorithm=TDES_2KEY,KeyUsage=TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS,KeyClass=SYMMETRIC_KEY,KeyMod
 --tags='[{"Key":"KEY_PURPOSE","Value":"CVN10"},{"Key":"CARD_BIN","Value":"12345678"}]'
```

La respuesta refleja los parámetros de la solicitud, incluyendo un ARN para las llamadas posteriores y un valor de verificación clave (KCV).

```
{
                        "Key": {
                            "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/pw3s6nl62t5ushfk",
                            "KeyAttributes": {
                                "KeyUsage": "TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS",
                                "KeyClass": "SYMMETRIC_KEY",
                                "KeyAlgorithm": "TDES_2KEY",
                                "KeyModesOfUse": {
                                    "Encrypt": false,
                                    "Decrypt": false,
                                    "Wrap": false,
                                    "Unwrap": false,
                                    "Generate": false,
                                    "Sign": false,
                                    "Verify": false,
                                    "DeriveKey": true,
                                    "NoRestrictions": false
                                }
                            },
                            "KeyCheckValue": "08D7B4",
                            "KeyCheckValueAlgorithm": "ANSI_X9_24",
                            "Enabled": true,
                            "Exportable": true,
                            "KeyState": "CREATE_COMPLETE",
```

```
                        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
                        "CreateTimestamp": "2024-03-07T06:41:46.648000-07:00",
                        "UsageStartTimestamp": "2024-03-07T06:41:46.626000-07:00"
                    }
                }
```

Tome nota de lo `KeyArn` que representa la clave, por ejemplo arn:aws:payment-cryptography:us-east- 2:111122223333:key/pw3s6nl62t5ushfk. Lo necesitará en el siguiente paso.

Valide el ARQC

Example

En este ejemplo, validaremos un ARQC generado con JCB. CVN01 Utiliza las mismas opciones que el método Visa, de ahí el nombre del parámetro.

Si la criptografía de AWS pagos es capaz de validar el ARQC, se devuelve un http/200. Si el arqc no se valida, devolverá una respuesta http/400.

```
$ aws payment-cryptography-data verify-auth-request-cryptogram --auth-request-
cryptogram D791093C8A921769 \
             --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk \
             --major-key-derivation-mode EMV_OPTION_A \
             --transaction-data
 00000000170000000000000008400080008000084016051700000000093800000B03011203000000 \
             --session-key-derivation-attributes='{"Visa":{"PanSequenceNumber":"01" \
             ,"PrimaryAccountNumber":"9137631040001422"}}'
```

```
{
                "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
pw3s6nl62t5ushfk",
                "KeyCheckValue": "08D7B4"
             }
```

Facilitadores de adquisiciones y pagos

Los adquirentes PSPs y los facilitadores de pagos suelen tener un conjunto de requisitos criptográficos diferentes a los de los emisores. Los casos de uso comunes incluyen:

Descifrado de datos

Los datos (especialmente los datos panorámicos) pueden estar cifrados por un terminal de pago y deben ser descifrados por el servidor. Decrypt Data y Encrypt Data admiten una variedad de métodos, incluidas las técnicas de derivación TDES, AES y DUKPT. El propio servicio AWS de criptografía de pagos también es compatible con PCI P2PE y está registrado como un componente de descifrado PCI P2PE.

TranslatePin

Para garantizar la conformidad con el PIN PCI, los sistemas de adquisición no deberán tener los pines de los titulares de las tarjetas en blanco después de haberlos introducido en un dispositivo seguro. Por lo tanto, para pasar el pin del terminal a un sistema posterior (como una red de pago o un emisor), es necesario volver a cifrarlo con una clave diferente a la que utilizó el terminal de pago. Translate Pin lo logra al convertir un pin cifrado de una clave a otra de forma segura con el servicio.bbb. Con este comando, los pines se pueden convertir entre varios esquemas, como la derivación TDES, AES y DUKPT, y entre formatos de bloques de pines, como el ISO-0, el ISO-3 y el ISO-4.

VerifyMac

Los datos de un terminal de pago pueden estar machacados para garantizar que no se hayan modificado durante el tránsito. Verifica el Mac y GenerateMac admite una variedad de técnicas que utilizan claves simétricas, incluidas las técnicas de derivación TDES, AES y DUKPT para su uso con el algoritmo 1 de la ISO-9797-1, el algoritmo 3 de la ISO-9797-1 (MAC minorista) y las técnicas de CMAC.

Temas adicionales

- Uso de claves dinámicas

Uso de claves dinámicas

Las claves dinámicas permiten utilizar claves de un solo uso o de uso limitado para operaciones criptográficas como`EncryptData`. Este flujo se puede utilizar cuando el material clave cambia con frecuencia (por ejemplo, en todas las transacciones con tarjeta) y se desea evitar la importación del material clave al servicio. Las claves de corta duración se pueden utilizar como parte de SoftPOS/MPOC u otras soluciones.

> **Note**
>
> Esto se puede utilizar en lugar del flujo típico de criptografía de AWS pagos, en el que las claves criptográficas se crean o importan al servicio y las claves se especifican mediante un alias o un arn de clave.

Las siguientes operaciones admiten las claves dinámicas:

- EncryptData
- DecryptData
- ReEncryptData
- TranslatePin

Descifrado de datos

El siguiente ejemplo muestra el uso de claves dinámicas junto con el comando decrypt. En este caso, el identificador de clave es la clave de empaquetado (KEK) que protege la clave de descifrado (que se proporciona en el parámetro wrapped-key en formato TR-31). La clave empaquetada será el objetivo principal de D0 si se utiliza con el comando de descifrado junto con un modo de uso de B o D.

Example

```
$ aws payment-cryptography-data decrypt-data --key-identifier
 arn:aws:payment-cryptography:us-east-2:111122223333:key/ov6icy4ryas4zcza
 --cipher-text 12341234123412341234123412341234123A --decryption-attributes
 'Symmetric={Mode=CBC,InitializationVector=1234123412341234}'   --wrapped-key
 WrappedKeyMaterial={"Tr31KeyBlock"="D0112D0TN00E0000B05A6E82D7FC68B95C84306634B0000DA4701BE9BC
```

```
{
   "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza",
   "KeyCheckValue": "0A3674",
   "PlainText": "2E138A746A0032023BEF5B85BA5060BA"
}
```

Traducir un pin

En el siguiente ejemplo, se muestra el uso de teclas dinámicas junto con el comando translate pin para convertir una clave dinámica en una clave de trabajo de adquisición semiestática (AWK). En este caso, el identificador de clave entrante es la clave de empaquetado (KEK) que protege la clave de cifrado de pines dinámicos (PEK) que se proporciona en el formato TR-31. La clave empaquetada debe ser el objetivo principal, `P0` junto con un modo de uso de B o D. El identificador de clave saliente es una clave del tipo `TR31_P0_PIN_ENCRYPTION_KEY` y un modo de uso de Encrypt=True, wrap=TRUE

Example

```
$ aws payment-cryptography-data translate-pin-data --encrypted-pin-block
 "C7005A4C0FA23E02" --incoming-translation-
attributes=IsoFormat0='{PrimaryAccountNumber=171234567890123}'
 --incoming-key-identifier alias/PARTNER1_KEK  --outgoing-key-
identifier alias/ACQUIRER_AWK_PEK --outgoing-translation-attributes
 IsoFormat0="{PrimaryAccountNumber=171234567890123}"  --incoming-wrapped-key
 WrappedKeyMaterial={"Tr31KeyBlock"="D0112P0TB00S0000EB5D8E63076313162B04245C8CE351C956EA4A16CC
```

```
{
   "PinBlock": "2E66192BDA390C6F",
   "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza",
   "KeyCheckValue": "0A3674"
}
```

Características específicas de la región para la criptografía AWS de pagos

Es posible que algunas funciones sean específicas de una región y no se utilicen de otro modo. Estas funciones se describen con más detalle en esta sección.

AS2805

La Norma de Australia 2805 (AS2805) es una norma para transferencias electrónicas de fondos que se utiliza principalmente para transacciones de pago con tarjeta. Su mantenimiento corre a cargo de Standards Australia. El estándar consta de 6 libros que cubren numerosos temas, desde el formato de los mensajes hasta los estándares de cifrado.

La parte 6 proporciona orientación sobre la gestión de claves, incluida host-to-host la comunicación y los requisitos criptográficos pertinentes, mientras que otros aspectos se tratan en otras partes. node-to-node Toda la criptografía de este estándar se basa actualmente en el TDES.

> **Note**
>
> AS2805 está disponible actualmente en la región ap-southeast-2. Se extenderá a más regiones en un futuro próximo.

AS2805 presenta una serie de diferencias en comparación con otras implementaciones, que se resumen a continuación.

Protección de claves

Se basa en variantes de teclas en lugar de en bloques de teclas, como en el TR-31/X9.143. AWS La criptografía de pagos almacena todas las claves como bloques de claves internamente, pero permite importarlas, exportarlas y calcularlas utilizando 05 variantes definidas. AS28

Claves unidireccionales

AS2805 exige el uso de teclas unidireccionales. Si ambos nodos necesitan generar códigos de autenticación de mensajes (MAC), utilizan dos claves.

Bloques de pines

AS2805 define una técnica de derivación de claves para claves de cifrado de pines únicas por transacción. Se puede utilizar en lugar de DUKPT. El esquema AS28 05 se basa en los datos de las transacciones (número de rastreo e importe de la transacción) en comparación con el uso del contador de transacciones por parte de DUKPT.

Validación del intercambio de claves

Define un proceso para validar la KEK antes de empezar a intercambiar claves de trabajo, como las teclas PIN. En otros esquemas, las KEK se intercambian con poca frecuencia y se validan mediante KCV.

AS2805 utiliza el concepto de variantes clave en lugar de bloques clave para garantizar que las claves solo se utilicen para el propósito previsto (y único). A continuación se muestra cómo la criptografía de AWS pagos mapea las variantes y los bloques de teclas al importar, exportar o realizar otras funciones criptográficas con claves.

AS2805 Tipo de clave	AWS Tipo de clave de criptografía de pago
TERMINAL_MAJOR_KEY_VARIANT_00	TR31_K0_KEY_CLAVE DE CIFRADO
PIN_ENCRYPTION_KEY_VARIANT_28	TR31_P0_PIN_ENCRYPTION_KEY
MENSAJE_AUTHENTICATION_KEY_ VARIANT_24	TR31_M0_ISO_16609_MAC_KEY
DATA_ENCRYPTION_KEY_VARIANT_22	TR31_D0_KEY_SYMMETRIC_DATA_ ENCRYPTION_KEY
VARIANT_MASK_82, VARIANT_MASK_82C0	Las opciones están disponibles como parte del proceso de validación de la KEK. Estos tipos de claves son efímeros y el servicio no los almacena.

Dados dos nodos, el nodo1 y el nodo2, los siguientes ejemplos son desde la perspectiva del nodo1. AWS La criptografía de pagos es compatible con APIs ambos lados del proceso.

Temas

- Intercambio de clave inicial (KEK)
- Validación de la KEK
- Creación y transmisión de claves de trabajo
- Exportación de claves de trabajo
- Traducción de pines
- Generación y validación de Mac

Intercambio de clave inicial (KEK)

En AS28 05, cada lado tiene su propia KEK. Las KEK se refieren a la clave del lado remitente que se utilizará siempre que el remitente necesite protect/wrap claves y las envíe al nodo 2. KEK (r) es la clave creada por el lado opuesto (node2).

> **Note**
>
> Estos términos son relativos: un lado crea una clave (lado emisor) y el otro lado la recibe. Por lo tanto KEY1, en el nodo 1 se denomina KEK (s) y en el nodo 2 se denomina KEK (r).

Las KEK de AS28 05 son siempre del tipo de clave = TR31 _K0_KEY_ENCRYPTION_KEY, ya que se utilizan para proteger criptogramas y no bloques de claves. Esto se corresponde con AS28 TERMINAL_MAJOR_KEY_VARIANT_00, tal como se define en 05 6.1

Pasos:

1. Crea una clave

   Cree una clave mediante la CreateKeyAPI. Creará una clave del tipo TR31 _K0_KEY_ENCRYPTION_KEY
2. Determine el método para intercambiar claves con el nodo 2

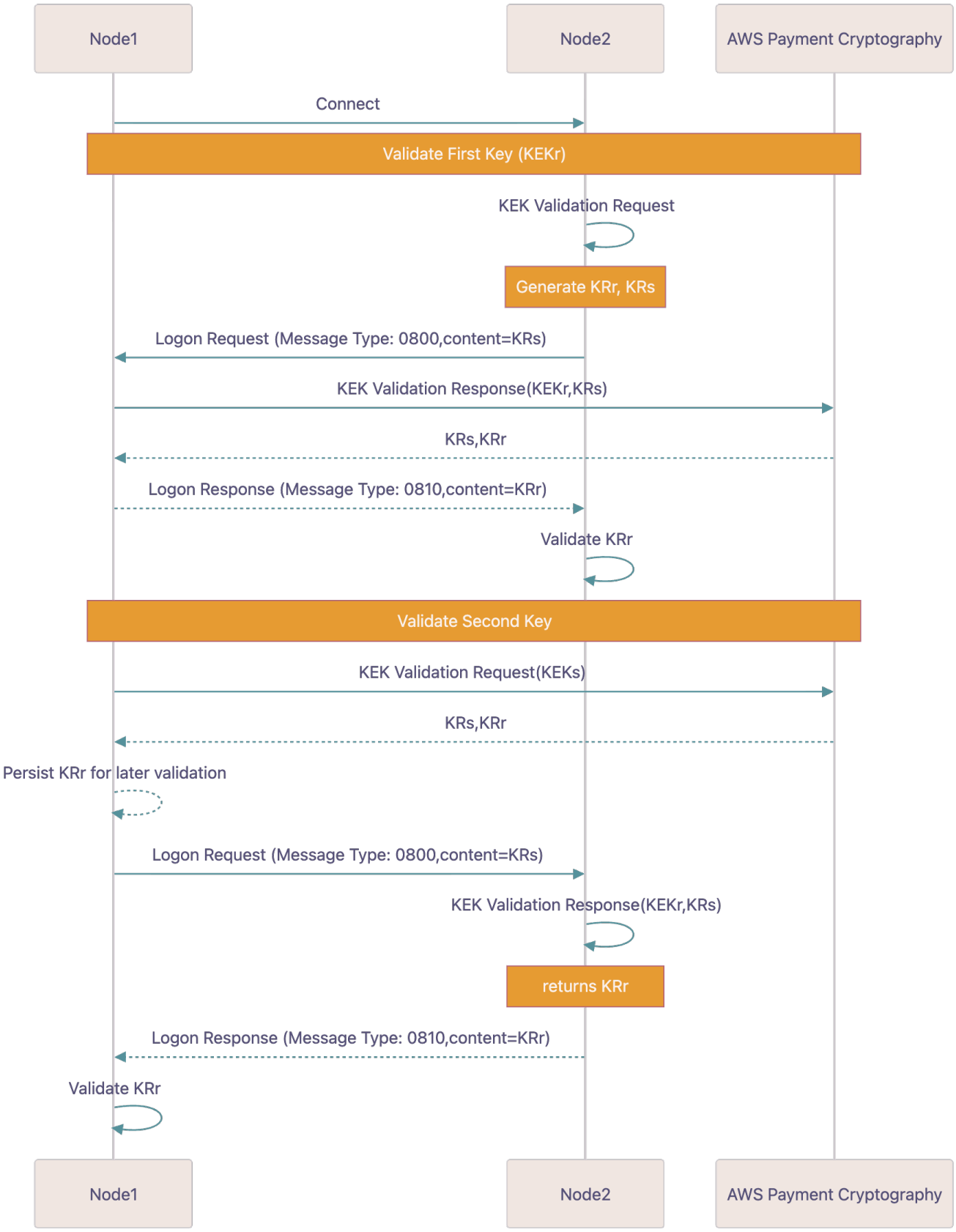
   Determine cómo intercambiar KEK con la contraparte. En el caso de AS28 05, el método más común e interoperable es RSA Wrap.
3. Exportar KEKs

   Según su selección anterior, recibirá un certificado de clave pública del nodo 2. Ejecutará la exportación con ese certificado para proteger la clave (o derivará una clave si utiliza el ECDH).

4. Importar KEKr

Según la selección anterior, enviará un certificado de clave pública a node2. Ejecutará la importación con ese certificado para cargar el nodo 2 KEKr en el servicio.

Validación de la KEK



Cuando su servicio (nodo1) se conecte al nodo2, cada parte se asegurará de utilizar la misma KEK para las operaciones posteriores mediante un proceso denominado validación de KEK.

1. Pasos para validar la primera clave

1.1 Recibir KRs

Node2 generará un mensaje KRs y se lo enviará como parte del proceso de inicio de sesión. Pueden usar la criptografía AWS de pago para generar este valor u otra solución.

1.2 Generar una respuesta de validación de KEK

El nodo generará una respuesta de validación de la KEK con entradas como la KEK (r) y las que KRs se proporcionan en el paso 1.

Example

```
cat >> generate-kek-validation-response.json
{
    "KekValidationType": {
        "KekValidationResponse": {
            "RandomKeySend": "9217DC67B8763BABCFDF3DADFCD0F84A"
        }
    },
    "RandomKeySendVariantMask": "VARIANT_MASK_82",
    "KeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza"
}
```

```
$ aws payment-cryptography-data generate-as2805-kek-validation --cli-input-json
 file://generate-kek-validation-response.json
```

```
{
 "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ov6icy4ryas4zcza",
 "KeyCheckValue": "0A3674",
 "RandomKeyReceive": "A4B7E249C40C98178C1B856DB7FB76EB",
 "RandomKeySend": "9217DC67B8763BABCFDF3DADFCD0F84A"
}
```

1.3 Retorno calculado KRr

Devuelve lo calculado KRr al nodo 2. Ese nodo lo comparará con el valor calculado en el paso 1.

2. Pasos para validar la segunda clave

2.1 Generar y KRr KRs

Su nodo generará un valor aleatorio y una copia invertida (invertida) de este valor mediante criptografía de AWS pago. El servicio generará ambos valores envueltos en las KEK. Se conocen como KR (s) y KR (r).

Example

```
cat >> generate-kek-validation-request.json
{
    "KekValidationType": {
        "KekValidationRequest": {
            "DeriveKeyAlgorithm": "TDES_2KEY"
        }
    },
"RandomKeySendVariantMask": "VARIANT_MASK_82",
    "KeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
rhfm6tenpxapkmrv"
}
```

```
$ aws payment-cryptography-data generate-as2805-kek-validation --cli-input-json
 file://generate-kek-validation-request.json
```

```
{
 "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
rhfm6tenpxapkmrv",
 "KeyCheckValue": "DC1081",
 "RandomKeyReceive": "A4B7E249C40C98178C1B856DB7FB76EB",
 "RandomKeySend": "9217DC67B8763BABCFDF3DADFCD0F84A"
}
```

2.2 Enviar KRs al nodo 2

Envíelo al nodo KRs 2. Consérvela KRr para su posterior validación.

2.3 El nodo 2 genera la respuesta de validación KEK

El nodo 2 usa la KEKr y KRs, la genera KRr y la envía de vuelta a su servicio.

2.4 Valida la respuesta

Compare el valor KRr del paso 1 con el valor devuelto en el paso 3. Si coinciden, proceda.

Creación y transmisión de claves de trabajo

Las teclas de trabajo típicas utilizadas en AS28 05 incluyen dos juegos de claves:

Claves entre nodos, como la clave PIN de zona (ZPK), la clave de cifrado de zona (ZEK) y la clave de autenticación de zona (ZAK).

Claves entre terminales y nodos, como la clave principal del terminal (TMK) y la clave PIN del terminal (TPK) si no se utiliza DUKPT.

> **Note**
>
> Recomendamos minimizar las llaves por terminal y utilizar técnicas como la TR-34 y la DUKPT, siempre que sea posible, que utilizan un número menor de teclas.

Example

En este ejemplo, hemos utilizado etiquetas opcionales para hacer un seguimiento del propósito y el uso de esta clave. Las etiquetas no se utilizan como parte de la función criptográfica del sistema, pero se pueden utilizar para la categorización, el seguimiento financiero y para aplicar políticas de IAM.

```
cat >> create-zone-pin-key.json
{
    "KeyAttributes": {
        "KeyUsage": "TR31_P0_PIN_ENCRYPTION_KEY",
        "KeyClass": "SYMMETRIC_KEY",
        "KeyAlgorithm": "TDES_2KEY",
        "KeyModesOfUse": {
            "Encrypt": true,
            "Decrypt": true,
            "Wrap": true,
            "Unwrap": true,
            "Generate": false,
            "Sign": false,
            "Verify": false,
            "DeriveKey": false,
            "NoRestrictions": false
        }
    },
    "KeyCheckValueAlgorithm": "ANSI_X9_24",
```

```
    "Exportable": true,
    "Enabled": true,
    "Tags": [
        {
            "Key": "AS2805_KEYTYPE",
            "Value": "ZONE_PIN_KEY_VARIANT28"
        }
    ]
}
```

```
$ aws payment-cryptography-data create-key --cli-input-json file://create-zone-pin-key.json --region ap-southeast-2
```

```
{
 "Key": {
 "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/alsuwfxug3pgy6xh",
 "KeyAttributes": {
 "KeyUsage": "TR31_P0_PIN_ENCRYPTION_KEY",
 "KeyClass": "SYMMETRIC_KEY",
 "KeyAlgorithm": "TDES_2KEY",
 "KeyModesOfUse": {
 "Encrypt": true,
 "Decrypt": true,
 "Wrap": true,
 "Unwrap": true,
 "Generate": false,
 "Sign": false,
 "Verify": false,
 "DeriveKey": false,
 "NoRestrictions": false
 }
 },
 "KeyCheckValue": "9A325B",
 "KeyCheckValueAlgorithm": "ANSI_X9_24",
 "Enabled": true,
 "Exportable": true,
 "KeyState": "CREATE_COMPLETE",
 "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
 "CreateTimestamp": "2025-12-17T09:05:27.586000-08:00",
 "UsageStartTimestamp": "2025-12-17T09:05:27.570000-08:00"
 }
}
```

Exportación de claves de trabajo

Para mantener la compatibilidad con otras partes, la criptografía de AWS pagos admite AS28 05 técnicas de empaquetado simétrico de claves que utilizan variantes de claves en lugar de bloques de teclas, como la TR-31. Si las partes comparten varias claves, cada una debe exportarse de forma individual. Si los datos se envían de forma bidireccional, es posible que haya dos claves entre partes del mismo tipo, como ZAK (s) y ZAK (r), que cada parte utilice para generar los códigos de autenticación de los mensajes.

Los parámetros adicionales para importar y exportar en estos formatos se especifican en los comandos.

```
cat >> export-zone-pin-key.json
{
    "ExportKeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh",
    "KeyMaterial": {
        "As2805KeyCryptogram": {
            "WrappingKeyIdentifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/rhfm6tenpxapkmrv",
            "As2805KeyVariant: "PIN_ENCRYPTION_KEY_VARIANT_28"
        }
    }
}
```

```
$ aws payment-cryptography-data export-key --cli-input-json file://export-zone-pin-
key.json --region ap-southeast-2
```

```
{
    "WrappedKey": {
        "KeyCheckValue": "DC1081",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyMaterial": "HDC10AEF038E695DDD72AF08DC1BB422D",
        "WrappedKeyMaterialFormat": "KEY_CRYPTOGRAM",
        "WrappingKeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
rhfm6tenpxapkmrv"
    }
}
```

Traducción de pines

AS2805 describe un modo de derivación de claves específico de la sesión en la sección 6.4. Tiene un propósito similar al DUKPT y se puede utilizar cualquiera de los dos algoritmos, ya que el DUKPT se describe en la sección 6.7. En este esquema, una clave PIN de sesión (conocida como KPE) se deriva de la clave PIN del terminal utilizando SystemTraceAuditNumber (STAN) y como datos de derivación. TransactionAmount

Translate pin es una función común que puede traducir to/from una variedad de formatos. En este ejemplo, traducimos un PIN de un KPE a una clave de cifrado de pines (PEK), como cuando enviamos un PIN a una red de pago.

```
cat >> translate-pin-as2805.json
{
    "EncryptedPinBlock": "B3B34B43BAB5F81A",
    "IncomingKeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
    "IncomingTranslationAttributes": {
        "IsoFormat0": {
            "PrimaryAccountNumber": "9999179999900013"
        }
    },
      "IncomingAs2805Attributes": {
        "SystemTraceAuditNumber": "000348",
        "TransactionAmount": "000000000328"
    },
    "OutgoingKeyIdentifier": "",
    "OutgoingTranslationAttributes": {
        "IsoFormat0": {
            "PrimaryAccountNumber": "9999179999900013"
        }
    }
}
```

```
$ aws payment-cryptography-data translate-pin-data --cli-input-json file://translate-
pin-as2805.json  --region ap-southeast-2
```

```
{
    "WrappedKey": {
        "KeyCheckValue": "DC1081",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
```

```
        "KeyMaterial": "HDC10AEF038E695DDD72AF08DC1BB422D",
        "WrappedKeyMaterialFormat": "KEY_CRYPTOGRAM",
        "WrappingKeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
rhfm6tenpxapkmrv"
    }
}
```

Generación y validación de Mac

Los comandos de generación y verificación de MAC admiten una variedad de comandos, MACs incluidos HMAC, CMAC, EMV MAC, etc. Para AS28 05, hay una variación adicional definida en la versión 05.4.1. AS28 Por lo general, en AS28 05, los mensajes entrantes se verifican con este MAC y los mensajes salientes también incluyen un MAC.

```
cat verify-mac.json
{
    "KeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6",
    "Mac": "86304058",
    "MessageData": "73D8BA54D3852951DAEA41",
    "VerificationAttributes": {
        "Algorithm": "AS2805_4_1"
    }
}
```

```
$ aws payment-cryptography-data verify-mac --cli-input-json file://verify-mac.json --
region ap-southeast-2
```

```
{
    "KeyIdentifier": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6",
    "KeyCheckValue": "2976E7"
}
```

Seguridad en la criptografía AWS de pagos

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube:AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a la criptografía de AWS pagos, consulte Servicios de AWS en el ámbito de aplicación por programa de conformidad .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Este tema le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar la criptografía AWS de pagos. Le muestra cómo configurar la criptografía AWS de pagos para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de criptografía AWS de pagos.

Temas

- La protección de datos en la criptografía AWS de pagos
- Resiliencia en la criptografía de pagos AWS
- Seguridad de infraestructura en AWS Payment Cryptography
- Conexión a la criptografía AWS de pagos a través de un punto final de VPC
- Usar el cifrado TLS híbrido postcuántico
- Prácticas recomendadas de seguridad para la criptografía AWS de pagos

La protección de datos en la criptografía AWS de pagos

El modelo de se aplica a la protección de datos en la criptografía AWS de pagos. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre privacidad de datos y los . Para obtener información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (GDPR).

Para proteger los datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con criptografía de AWS pagos u otro tipo Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear

para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

AWS Payment Cryptography almacena y protege sus claves de cifrado de pagos para que estén altamente disponibles al mismo tiempo que le proporciona un control de acceso sólido y flexible.

Temas

- Rotación del material de claves
- Cifrado de datos
- Cifrado en reposo
- Cifrado en tránsito
- Privacidad del tráfico entre redes

Rotación del material de claves

Por defecto, AWS Payment Cryptography protege el material criptográfico de las claves de pago gestionadas por el servicio. Además, AWS Payment Cryptography ofrece opciones para importar material de claves creado fuera del servicio. Para obtener más detalles sobre las claves de pago y el material de claves, consulte los detalles de criptografía de AWS Payment Cryptography.

Cifrado de datos

Los datos de AWS Payment Cryptography consisten en claves de AWS Payment Cryptography, el material de claves criptográficas que representan y sus atributos de uso. El material de claves solo existe en texto sin formato dentro de los módulos de seguridad de hardware (HSM) de AWS Payment Cryptography y solo cuando estén en uso. De lo contrario, el material de la clave y los atributos se cifran y se almacenan en almacenamiento persistente duradero.

El material de claves que AWS Payment Cryptography genera o carga para las claves de pago nunca abandona el límite de los HSM de AWS Payment Cryptography sin cifrar. Puede ser exportado cifrado por las operaciones API de AWS Payment Cryptography.

Cifrado en reposo

La criptografía de pagos de AWS genera material clave para las claves de pago en los HSM PCI PTS HSM-listed . Cuando no se utiliza, el material de claves se cifra mediante una clave de HSM

y se escribe en un almacenamiento duradero y persistente. El material de las claves de Payment Cryptography y las claves de cifrado que protegen el material de claves nunca dejan los HSM en forma de texto sin formato.

El cifrado y la administración del material de claves para las claves de Payment Cryptography está completamente a cargo del servicio.

Para obtener más información, consulte el documento técnico Detalles criptográficos de AWS Key Management Service.

Cifrado en tránsito

El material clave que la criptografía de AWS pagos genera o carga para las claves de pago nunca se exporta ni transmite en las operaciones de la API de criptografía de AWS pagos en texto claro. AWS La criptografía de pagos utiliza identificadores clave para representar las claves en las operaciones de la API.

Sin embargo, algunas operaciones de API exportan claves cifradas mediante una clave de intercambio de claves previamente compartida o asimétrica. Además, los clientes pueden usar las operaciones de la API para importar material de claves encriptadas para las claves de pago.

Todas las llamadas a la API de criptografía de AWS pagos deben firmarse y transmitirse mediante Transport Layer Security (TLS). AWS La criptografía de pagos requiere versiones TLS y conjuntos de cifrado definidos por PCI como «criptografía sólida». Todos los terminales de servicio admiten el TLS 1.2—1.3 y el TLS poscuántico híbrido.

Para obtener más información, consulte el documento técnico Detalles criptográficos de AWS Key Management Service.

Privacidad del tráfico entre redes

AWS La criptografía de pagos admite una consola de administración de AWS y un conjunto de operaciones de API que le permiten crear y administrar claves de pago y utilizarlas en operaciones criptográficas.

AWS La criptografía de pagos admite dos opciones de conectividad de red desde su red privada a AWS.

- Una conexión de una conexión de VPN IPSec a través de Internet.

- AWS Direct Connect vincula su red interna con una ubicación de AWS Direct Connect a través de cable estándar Ethernet de fibra óptica.

Todas las llamadas de la API de Payment Cryptography deben firmarse y transmitirse mediante seguridad de la capa de transporte (TLS). Las llamadas también requieren un paquete de cifrado moderno que admita el secreto perfecto en el futuro. El tráfico a los módulos de seguridad de hardware (HSM) que almacenan material de claves para las claves de pago solo se permite desde hosts de la API de AWS Payment Cryptography a través de la red interna de AWS.

Para conectarse directamente a la criptografía de pagos de AWS desde su nube privada virtual (VPC) sin enviar tráfico a través de la Internet pública, utilice los puntos de enlace de VPC, con tecnología de AWS. PrivateLink Para obtener más información, consulte Conexión a AWS Payment Cryptography a través de un punto de conexión de VPC.

AWS Payment Cryptography admite también una opción de intercambio híbrido postcuántico de claves para el protocolo de cifrado de red de seguridad de la capa de transporte (TLS). Puede utilizar esta opción de TLS cuando se conecte a los puntos de conexión de la API de AWS Payment Cryptography.

Resiliencia en la criptografía de pagos AWS

AWS La infraestructura global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Aislamiento regional

La criptografía de pagos de AWS es un servicio regional que está disponible en varias regiones.

El diseño regionalmente aislado de AWS Payment Cryptography garantiza que un problema de disponibilidad en una región de AWS no puede afectar al funcionamiento de AWS Payment

Cryptography en ninguna otra región. AWS Payment Cryptography está diseñado para garantizar un tiempo de inactividad planificado cero, con todas las actualizaciones de software y operaciones de escalado realizadas de manera imperceptible y sin problemas.

El Acuerdo de nivel de servicio (SLA) de AWS Payment Cryptography incluye un compromiso de servicio del 99,99 % para todas las API de AWS Payment Cryptography. Para cumplir este compromiso, AWS Payment Cryptography garantiza que todos los datos y la información de autorización necesarios para ejecutar una solicitud de la API estén disponibles en todos los hosts regionales que reciben la solicitud.

La infraestructura de AWS Payment Cryptography se replica en al menos tres zonas de disponibilidad (AZ) en cada región. Para garantizar que los errores de varios hosts no afecten al rendimiento, AWS Payment Cryptography está diseñado para atender el tráfico de clientes de cualquiera de las zonas de disponibilidad de una región.

Los cambios realizados en las propiedades o permisos de una clave de pagos se replican en todos los hosts de la región para garantizar que cualquier host de la región pueda procesar de manera correcta la solicitud posterior. Solicitudes de operaciones criptográficas mediante el uso de la clave de pagos se reenvían a una flota de módulos de seguridad de hardware (HSM) de AWS Payment Cryptography, cualquiera de los cuales puede realizar la operación con la clave de pagos.

Multi-tenant diseño

El diseño de varios inquilinos de AWS Payment Cryptography permite cumplir el SLA de disponibilidad y mantener altas tasas de solicitudes, al tiempo que protege la confidencialidad de las claves y los datos.

Se implementan varios mecanismos de cumplimiento de la integridad para garantizar que la clave de pagos especificada para la operación criptográfica sea siempre la que se utiliza.

El material de clave de texto sin formato para las claves de Payment Cryptography está ampliamente protegido. El material de clave se cifra en el HSM tan pronto como se crea y el material de clave cifrado se mueve de inmediato al almacenamiento seguro. La clave cifrada se recupera y se descifra dentro del HSM justo a tiempo para su uso. La clave de texto sin formato permanece en la memoria HSM solo durante el tiempo necesario para completar la operación criptográfica. El material de claves de texto sin formato nunca sale de los HSM; nunca se escribe en un almacenamiento persistente.

Para obtener más información acerca de los mecanismos que AWS Payment Cryptography utiliza para proteger sus claves, consulte Detalles criptográficos de AWS Payment Cryptography.

Seguridad de infraestructura en AWS Payment Cryptography

Como servicio gestionado, AWS Payment Cryptography está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Payment Cryptography través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o con una versión posterior. Los clientes también deben admitir conjuntos de cifrado con perfecto secreto directo (PFS), como Ephemeral (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de hosts físicos

La seguridad de la infraestructura física que AWS Payment Cryptography utiliza está sujeto a los controles que se describen en la sección Seguridad Física y Ambiental de Amazon Web Services: Información general de los procesos de seguridad. Puede encontrar más detalles en los informes de conformidad y los resultados de auditoría de terceros enumerados en la sección anterior.

La criptografía de pagos de AWS está respaldada por módulos de seguridad de HSM-listed hardware (HSM) PCI PTS específicos y listos para usar en el mercado. El material de claves para las claves de AWS Payment Cryptography se almacena solo en memoria volátil en los HSM, y solo mientras la clave de Payment Cryptography está en uso. Los HSM se encuentran en bastidores de acceso controlado dentro de los centros de datos de Amazon que aplican un doble control para cualquier acceso físico. Para obtener información detallada acerca de la operación de los HSM de AWS Payment Cryptography, consulte Detalles criptográficos de AWS Payment Cryptography.

Conexión a la criptografía AWS de pagos a través de un punto final de VPC

Puede conectarse directamente a la criptografía de AWS pagos a través de un punto final de interfaz privada en su nube privada virtual (VPC). Cuando utiliza un punto final de VPC de interfaz, la

comunicación entre su VPC y la criptografía de AWS pagos se lleva a cabo íntegramente dentro de la red. AWS

AWS La criptografía de pagos es compatible con los puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC) con la tecnología de. AWS PrivateLink Cada punto de conexión de VPC está representado por una o varias Interfaces de red elásticas (ENI) con direcciones IP privadas en las subredes de la VPC.

El punto final de la interfaz VPC conecta su VPC directamente a la criptografía de AWS pagos sin necesidad de una pasarela de Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con AWS Payment Cryptography.

Regions

AWS La criptografía de pagos es compatible con los puntos de enlace de VPC y las políticas de puntos de enlace de VPC Regiones de AWS AWS en todos los que se admite la criptografía de pagos.

Temas

- Consideraciones sobre los puntos AWS finales de VPC de criptografía de pagos
- Creación de un punto final de VPC para AWS criptografía de pagos
- Conexión a un punto final de AWS VPC de criptografía de pagos
- Control del acceso a un punto de conexión de VPC
- Utilizar un punto de conexión de VPC en una declaración de política
- Registro de su punto de conexión de VPC

Consideraciones sobre los puntos AWS finales de VPC de criptografía de pagos

> **Note**
>
> Si bien los puntos de enlace de la VPC le permiten conectarse al servicio en tan solo una zona de disponibilidad (AZ), le recomendamos que se conecte a tres zonas de disponibilidad por motivos de alta disponibilidad y redundancia.

Antes de configurar un punto final de la VPC de la interfaz para la criptografía de AWS pagos, consulte el tema de propiedades y limitaciones del punto final de la interfaz en la Guía.AWS PrivateLink

AWS El soporte de criptografía de pagos para un punto final de VPC incluye lo siguiente.

- Puede usar su punto final de VPC para llamar a todas las operaciones del plano de control de criptografía de AWS pagos y las operaciones del plano de datos de criptografía de AWS pagos desde una VPC.
- Puede crear un punto final de VPC de interfaz que se conecte a un punto final de la región de criptografía AWS de pagos.
- AWS La criptografía de pagos consta de un plano de control y un plano de datos. Puede elegir configurar uno o ambos subservicios, AWS PrivateLink pero cada uno se configura por separado.
- Puedes usar AWS CloudTrail los registros para auditar tu uso de las claves de criptografía de AWS pago a través del punto final de la VPC. Para obtener más información, consulte Registro de su punto de conexión de VPC.

Creación de un punto final de VPC para AWS criptografía de pagos

Puede crear un punto de conexión de VPC para la criptografía de AWS pagos mediante la consola de Amazon VPC o la API de Amazon VPC. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

- Para crear un punto final de VPC para la criptografía AWS de pagos, utilice los siguientes nombres de servicio:

```
com.amazonaws.region.payment-cryptography.controlplane
```

```
com.amazonaws.region.payment-cryptography.dataplane
```

  Por ejemplo, en la región EE.UU. Oeste (Oregón) (`us-west-2`), los nombres de los servicios serían:

```
com.amazonaws.us-west-2.payment-cryptography.controlplane
```

```
com.amazonaws.us-west-2.payment-cryptography.dataplane
```

Para facilitar el uso del punto de conexión de VPC, puede habilitar un nombre de DNS privado para el punto de conexión de VPC. Si selecciona la opción Habilitar nombre DNS, el nombre de host DNS de criptografía de AWS pagos estándar se transfiere a su punto final de VPC. Por ejemplo, `https://controlplane.payment-cryptography.us-west-2.amazonaws.com` se resolvería en un punto de conexión de VPC conectado al nombre del servicio `com.amazonaws.us-west-2.payment-cryptography.controlplane`.

Esta opción facilita el uso del punto de conexión de VPC. AWS Los SDK y Payment Cryptography AWS CLI utilizan el nombre de host DNS estándar de criptografía de AWS pagos de forma predeterminada, por lo que no es necesario especificar la URL del punto final de la VPC en las aplicaciones y comandos.

Para obtener más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Conexión a un punto final de AWS VPC de criptografía de pagos

Puede conectarse a la criptografía AWS de pagos a través del punto final de la VPC mediante AWS un SDK, AWS CLI el o. Herramientas de AWS para PowerShell Para especificar el punto de conexión de VPC, utilice su nombre de DNS.

Por ejemplo, este comando list-keys utiliza el parámetro `endpoint-url` para especificar el punto de conexión de VPC. Para utilizar un comando de este tipo, sustituya el ID del punto de conexión de VPC del ejemplo por uno de su cuenta.

```
$ aws payment-cryptography list-keys --endpoint-url https://
vpce-1234abcdf5678c90a-09p7654s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com
```

Si ha habilitado los nombres de host privados al crear el punto de conexión de VPC, no es necesario que especifique la URL de este en los comandos de la CLI ni en la configuración de la aplicación. El nombre de host DNS AWS de criptografía de pagos estándar se resuelve en el punto final de la VPC. Los SDK AWS CLI y utilizan este nombre de host de forma predeterminada, por lo que puedes empezar a utilizar el punto de enlace de la VPC para conectarte a un punto de conexión regional de criptografía de AWS pagos sin cambiar nada en tus scripts y aplicaciones.

Para utilizar nombres de host privados, se deben establecer los atributos `enableDnsHostnames` y `enableDnsSupport` de la VPC en `true`. Para configurar estos atributos, usa la operación. ModifyVpcAttribute Para obtener más información, consulte Ver y actualizar los atributos de DNS de su VPC en la Guía del usuario de Amazon VPC.

Control del acceso a un punto de conexión de VPC

Para controlar el acceso a su punto final de VPC para la criptografía de AWS pagos, adjunte una política de punto final de VPC a su punto de enlace de VPC. La política de puntos finales determina si los principales pueden usar el punto final de la VPC para AWS llamar a las operaciones de criptografía de pagos con recursos de criptografía de pagos AWS específicos.

Puede crear una política de punto de conexión de VPC cuando cree el punto de conexión y puede cambiar la política de punto de conexión de VPC en cualquier momento. Utilice la consola de administración de VPC o las operaciones CreateVpcEndpointo ModifyVpcEndpoint. También puede crear y cambiar una política de puntos finales de VPC mediante una AWS CloudFormation plantilla. Para obtener ayuda sobre el uso de la consola de administración de la VPC, consulte Creación de un punto de conexión de interfaz y Modificación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Para obtener ayuda sobre cómo escribir y dar formato a un documento de política JSON, consulte la Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Temas

- Uso de políticas de punto de conexión de VPC
- Política de puntos de conexión de VPC predeterminada
- Creación de una política de punto de conexión de VPC
- Visualización de una política de punto de conexión de VPC

Uso de políticas de punto de conexión de VPC

Para que una solicitud de criptografía de AWS pagos que utilice un punto final de VPC se lleve a cabo correctamente, el director necesita permisos de dos fuentes:

- Una política basada en la identidad debe conceder al principal permiso para realizar la operación en el recurso (claves o alias de criptografía AWS de pagos).
- Una política de extremo de VPC debe conceder a la entidad principal permiso para utilizar el punto de conexión para realizar la solicitud.

Por ejemplo, una política clave puede conceder a un director permiso para llamar a Decrypt en una determinada AWS clave de criptografía de pago. Sin embargo, es posible que la política de puntos

finales de la VPC no permita que el principal invoque `Decrypt` esas claves de criptografía de AWS pagos mediante el punto final.

O bien, una política de puntos finales de la VPC podría permitir que un principal utilice el punto final para solicitar determinadas claves StopKeyUsagede criptografía AWS de pagos. Sin embargo, si el principal no tiene esos permisos de una política de IAM, la solicitud no se realizará correctamente.

Política de puntos de conexión de VPC predeterminada

Cada punto de conexión de VPC tiene una política de punto de conexión de VPC, pero no es necesario que especifique la política. Si no especifica una política, la política de punto de conexión predeterminada permite todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión.

Sin embargo, en el caso de los recursos de criptografía de AWS pagos, el director también debe tener permiso para llamar a la operación desde una política de IAM. Por lo tanto, en la práctica, la política predeterminada dice que si una entidad principal tiene permiso para llamar a una operación en un recurso, también puede llamarla mediante el punto de conexión.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Para permitir que las entidades principales utilicen el punto de conexión de VPC solo para un subconjunto de sus operaciones permitidas, cree o modifique la política de puntos de conexión de VPC.

Creación de una política de punto de conexión de VPC

Una política de punto de conexión de VPC determina si una entidad principal tiene permiso para utilizar el punto de conexión de VPC para realizar operaciones en un recurso. En el AWS caso de los recursos de criptografía de pagos, el principal también debe tener permiso para realizar las operaciones en virtud de una política de IAM.

Cada declaración de política de puntos de conexión de VPC requiere los siguientes elementos:

- La entidad principal que puede realizar acciones
- Las acciones que se pueden realizar
- Los recursos en los que se pueden llevar a cabo las acciones

La declaración de política no especifica el punto de conexión de VPC. En cambio, se aplica a cualquier punto de conexión de VPC al que esté asociada dicha política. Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la guía del usuario de Amazon VPC.

El siguiente es un ejemplo de una política de punto final de VPC para criptografía de AWS pagos. Cuando se conecta a un punto final de la VPC, esta política permite usar el punto final de la VPC `ExampleUser` para llamar a las operaciones especificadas en las claves de criptografía de pago especificadas AWS . Antes de utilizar una política como esta, sustituya el identificador principal y clave del ejemplo por valores válidos de su cuenta.

```
{
   "Statement":[
      {
         "Sid": "AllowDecryptAndView",
         "Principal": {"AWS": "arn:aws:iam::111122223333:user/ExampleUser"},
         "Effect":"Allow",
         "Action": [
             "payment-cryptography:Decrypt",
             "payment-cryptography:GetKey",
             "payment-cryptography:ListAliases",
             "payment-cryptography:ListKeys",
             "payment-cryptography:GetAlias"
          ],
         "Resource": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h"
      }
   ]
}
```

AWS CloudTrail registra todas las operaciones que utilizan el punto final de la VPC. Sin embargo, tus CloudTrail registros no incluyen las operaciones solicitadas por los responsables de otras cuentas ni las operaciones relacionadas con las claves de criptografía de AWS pagos de otras cuentas.

Por lo tanto, es posible que desee crear una política de punto final de la VPC que impida que los directores de las cuentas externas utilicen el punto de enlace de la VPC para realizar cualquier operación de criptografía de AWS pagos en cualquier clave de la cuenta local.

En el siguiente ejemplo, se utiliza la clave de condición aws: PrincipalAccount global para denegar el acceso a todos los principales para todas las operaciones con todas las claves de criptografía de AWS pagos, a menos que el principal esté en la cuenta local. Antes de utilizar una política como esta, sustituya el ID de la cuenta de ejemplo por uno válido.

```
{
  "Statement": [
    {
      "Sid": "AccessForASpecificAccount",
      "Principal": {"AWS": "*"},
      "Action": "payment-cryptography:*",
      "Effect": "Deny",
      "Resource": "arn:aws:payment-cryptography:*:111122223333:key/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Visualización de una política de punto de conexión de VPC

Para ver la política de puntos de conexión de la VPC de un punto final, utilice la consola de administración de la VPC o la operación. DescribeVpcEndpoints

El siguiente AWS CLI comando obtiene la política del punto final con el ID de punto final de VPC especificado.

Antes de ejecutar este comando, reemplace el ID de punto de conexión de ejemplo por uno válido de su cuenta.

```
$ aws ec2 describe-vpc-endpoints \
--query 'VpcEndpoints[?VpcEndpointId==`vpce-1234abcdf5678c90a`].[PolicyDocument]'
--output text
```

Utilizar un punto de conexión de VPC en una declaración de política

Puede controlar el acceso a los recursos y las operaciones de criptografía de AWS pagos cuando la solicitud proviene de la VPC o utiliza un punto final de la VPC. Para ello, utilice una política de IAM

- Utilice la clave de condición `aws:sourceVpce` para conceder o restringir el acceso en función del punto de conexión de VPC.
- Utilice la clave de condición `aws:sourceVpc` para conceder o restringir el acceso en función de la VPC que aloja el punto de conexión privado.

> **Note**
>
> La clave de `aws:sourceIP` condición no entra en vigor cuando la solicitud proviene de un punto de conexión de Amazon VPC. Para restringir las solicitudes a un punto de conexión de VPC, utilice las claves de condición `aws:sourceVpce` o `aws:sourceVpc`. Para obtener más información, consulte Administración de identidades y accesos para puntos de conexión de VPC y servicios de puntos de conexión de VPC en la Guía de AWS PrivateLink .

Puede utilizar estas claves de condición globales para controlar el acceso a las claves de criptografía de AWS pagos, a los alias y a operaciones de CreateKeyeste tipo que no dependen de ningún recurso en particular.

Por ejemplo, el siguiente ejemplo de política de claves permite a un usuario realizar determinadas operaciones criptográficas con claves de criptografía de AWS pago solo cuando la solicitud utiliza el punto final de VPC especificado, lo que bloquea el acceso tanto desde Internet como desde las AWS PrivateLink conexiones (si está configurado). Cuando un usuario realiza una solicitud a AWS Payment Cryptography, el ID del punto final de la VPC de la solicitud se compara con el valor de `aws:sourceVpce` la clave de condición de la política. Si no coinciden, la solicitud se deniega.

Para usar una política como esta, sustituya el ID del marcador de posición y los Cuenta de AWS ID de punto final de la VPC por valores válidos para su cuenta.

JSON

```
{
    "Id": "example-key-1",
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EnableIAMPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root"
                ]
            },
            "Action": [
                "payment-cryptography:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RestrictUsageToMyVPCEndpoint",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "payment-cryptography:EncryptData",
                "payment-cryptography:DecryptData"
            ],
            "Resource": "arn:aws:payment-cryptography:us-east-1:111122223333:key/
*",
            "Condition": {
                "StringNotEquals": {
                    "aws:sourceVpce": "vpce-1234abcdf5678c90a"
                }
            }
        }

    ]
}
```

También puede usar la clave de `aws:sourceVpc` condición para restringir el acceso a sus claves de criptografía de AWS pagos en función de la VPC en la que reside el punto final de la VPC.

El siguiente ejemplo de política de claves permite que los comandos gestionen las claves de criptografía de AWS pagos solo cuando proceden de ellas. `vpc-12345678` Además, permite ejecutar comandos que utilicen las claves de criptografía de AWS pagos para operaciones criptográficas únicamente cuando procedan de. `vpc-2b2b2b2b` Podría utilizar una política como

esta en caso de que una aplicación se ejecute en una VPC, pero utiliza una segunda VPC aislada para funciones de administración.

Para usar una política como esta, sustituya el ID del marcador de posición y los Cuenta de AWS ID de punto final de la VPC por valores válidos para su cuenta.

JSON

```
{
    "Id": "example-key-2",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAdminActionsFromVPC12345678",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
               "payment-cryptography:Create*",
               "payment-cryptography:Encrypt*",
               "payment-cryptography:ImportKey*",
               "payment-cryptography:GetParametersForImport*",
               "payment-cryptography:TagResource",
               "payment-cryptography:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpc": "vpc-12345678"
                }
            }
        },
        {
            "Sid": "AllowKeyUsageFromVPC2b2b2b2b",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
                "payment-cryptography:Encrypt*",
                "payment-cryptography:Decrypt*"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpc": "vpc-2b2b2b2b"
                }
            }
        },
        {
            "Sid": "AllowListReadActionsFromEverywhere",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
                "payment-cryptography:List*",
                "payment-cryptography:Get*"
            ],
            "Resource": "*"
        }
    ]
}
```

Registro de su punto de conexión de VPC

AWS CloudTrail registra todas las operaciones que utilizan el punto final de la VPC. Cuando una solicitud a AWS Payment Cryptography utiliza un punto de enlace de VPC, el ID del punto de enlace de VPC aparece en AWS CloudTrail la entrada de registro que registra la solicitud. Puede usar el ID del punto final para auditar el uso de su punto final de VPC de criptografía de AWS pagos.

Para proteger su VPC, no se registran las solicitudes denegadas por una política de puntos finales de la VPC, pero que de otro modo se habrían permitido. AWS CloudTrail

Por ejemplo, esta entrada de log de ejemplo registra una solicitud GenerateMac que ha utilizado el punto de enlace de la VPC. El campo `vpcEndpointId` aparece al final de la entrada de log.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
          "principalId": "TESTXECZ5U9M4LGF2N6Y5:i-98761b8890c09a34a",
          "arn": "arn:aws:sts::111122223333:assumed-role/samplerole/
i-98761b8890c09a34a",
```

```
            "accountId": "111122223333",
            "accessKeyId": "TESTXECZ5U2ZULLHHMJG",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "TESTXECZ5U9M4LGF2N6Y5",
                    "arn": "arn:aws:iam::111122223333:role/samplerole",
                    "accountId": "111122223333",
                    "userName": "samplerole"
                },
                "webIdFederationData": {},
                "attributes": {
                    "creationDate": "2024-05-27T19:34:10Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2024-05-27T19:49:54Z",
        "eventSource": "payment-cryptography.amazonaws.com",
        "eventName": "CreateKey",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "172.31.85.253",
        "userAgent": "aws-cli/2.14.5 Python/3.9.16 Linux/6.1.79-99.167.amzn2023.x86_64
    source/x86_64.amzn.2023 prompt/off command/payment-cryptography.create-key",
        "requestParameters": {
            "keyAttributes": {
                "keyUsage": "TR31_M1_ISO_9797_1_MAC_KEY",
                "keyClass": "SYMMETRIC_KEY",
                "keyAlgorithm": "TDES_2KEY",
                "keyModesOfUse": {
                    "encrypt": false,
                    "decrypt": false,
                    "wrap": false,
                    "unwrap": false,
                    "generate": true,
                    "sign": false,
                    "verify": true,
                    "deriveKey": false,
                    "noRestrictions": false
                }
            },
            "exportable": true
        },
```

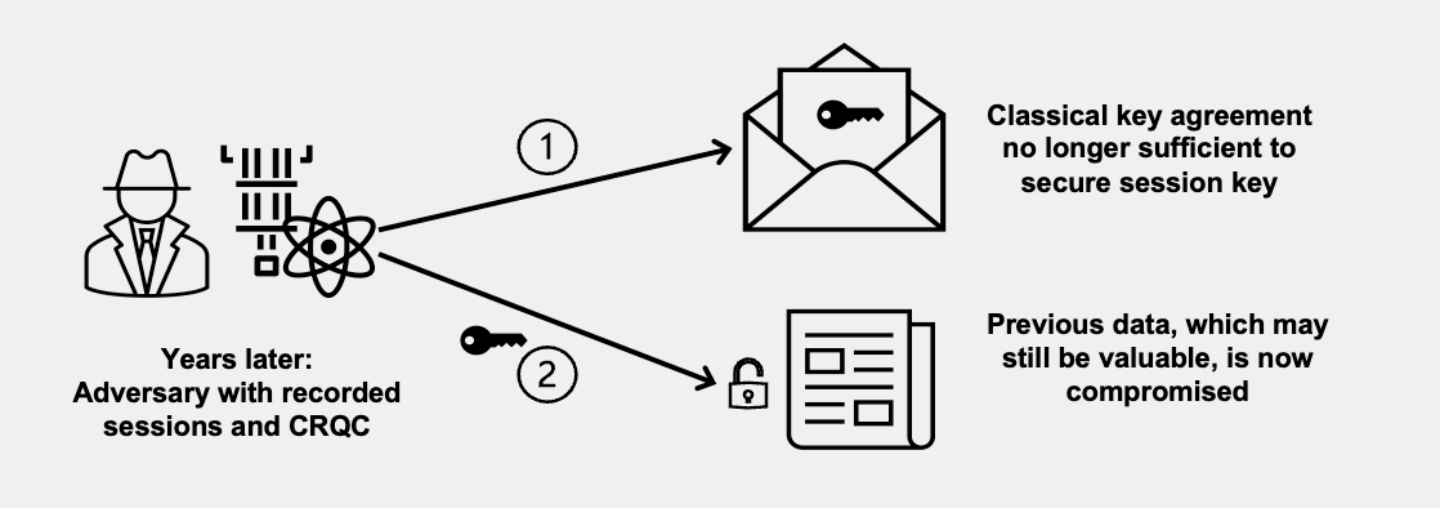
```
      "responseElements": {
          "key": {
              "keyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h",
              "keyAttributes": {
                  "keyUsage": "TR31_M1_ISO_9797_1_MAC_KEY",
                  "keyClass": "SYMMETRIC_KEY",
                  "keyAlgorithm": "TDES_2KEY",
                  "keyModesOfUse": {
                      "encrypt": false,
                      "decrypt": false,
                      "wrap": false,
                      "unwrap": false,
                      "generate": true,
                      "sign": false,
                      "verify": true,
                      "deriveKey": false,
                      "noRestrictions": false
                  }
              },
              "keyCheckValue": "A486ED",
              "keyCheckValueAlgorithm": "ANSI_X9_24",
              "enabled": true,
              "exportable": true,
              "keyState": "CREATE_COMPLETE",
              "keyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
              "createTimestamp": "May 27, 2024, 7:49:54 PM",
              "usageStartTimestamp": "May 27, 2024, 7:49:54 PM"
          }
      },
      "requestID": "f3020b3c-4e86-47f5-808f-14c7a4a99161",
      "eventID": "b87c3d30-f3ab-4131-87e8-bc54cfef9d29",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "vpcEndpointId": "vpce-1234abcdf5678c90a",
      "eventCategory": "Management",
      "tlsDetails": {
          "tlsVersion": "TLSv1.3",
          "cipherSuite": "TLS_AES_128_GCM_SHA256",
          "clientProvidedHostHeader": "vpce-1234abcdf5678c90a-
oo28vrvr.controlplane.payment-cryptography.us-east-1.vpce.amazonaws.com"
      }
```

```
}
```

Usar el cifrado TLS híbrido postcuántico

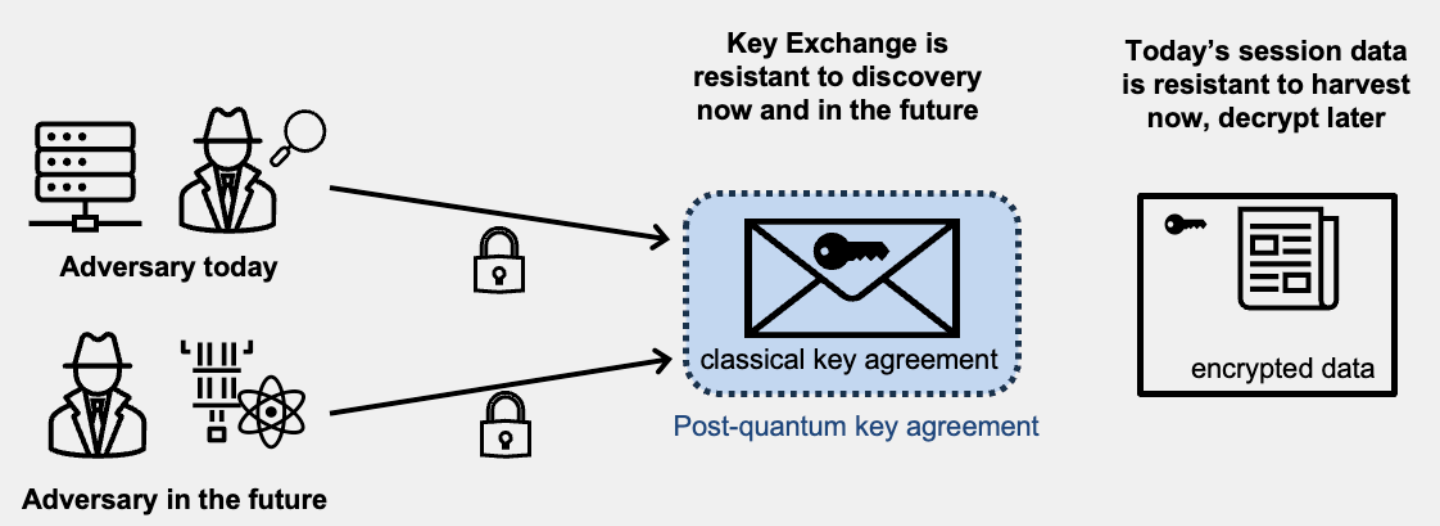
AWS La criptografía de pagos y muchos otros servicios admiten una opción híbrida de intercambio de claves poscuántico para el protocolo de cifrado de red Transport Layer Security (TLS). Puede utilizar esta opción de TLS cuando se conecte a los puntos de enlace de la API o cuando utilice los SDK de AWS. Estas características opcionales de intercambio híbrido postcuántico de claves son al menos tan seguras como el cifrado TLS que utilizamos hoy en día y es muy probable que aporten beneficios de seguridad adicionales.

Los datos que envíe a los servicios habilitados están protegidos en tránsito mediante el cifrado que proporciona una conexión de Transport Layer Security (TLS). Los conjuntos de cifrado clásicos basados en RSA y ECC que AWS Payment Cryptography admite para las sesiones de TLS hacen que los ataques de fuerza bruta a los mecanismos de intercambio de claves no sean factibles con la tecnología actual. Sin embargo, si las computadoras cuánticas a gran escala o criptográficamente relevantes (CRQC) se vuelven prácticas en el futuro, los mecanismos de intercambio de claves TLS existentes serán susceptibles a estos ataques. Es posible que los adversarios comiencen a recolectar datos cifrados ahora con la esperanza de poder descifrarlos en el futuro (recolectarlos ahora, desencriptarlos más tarde). Si está desarrollando aplicaciones que se basan en la confidencialidad a largo plazo de los datos transmitidos a través de una conexión TLS, debería plantearse un plan para migrar a la criptografía poscuántica antes de que se puedan utilizar ordenadores cuánticos a gran escala. AWS está trabajando para prepararse para este futuro y queremos que usted también esté bien preparado.



Para proteger los datos cifrados hoy contra posibles ataques futuros, AWS participa con la comunidad criptográfica en el desarrollo de algoritmos cuánticos resistentes o poscuánticos. AWS ha implementado conjuntos de cifrado híbridos de intercambio de claves poscuántico que combinan elementos clásicos y poscuánticos para garantizar que su conexión TLS sea al menos tan sólida como lo sería con los conjuntos de cifrado clásicos.

Estos conjuntos de cifrado híbridos están disponibles para su uso en sus cargas de trabajo de producción cuando utilice versiones recientes de los SDK de AWS. Para obtener más información sobre cómo se produce enable/disable este comportamiento, consulte ???



Acerca del intercambio de claves postcuántico híbrido en TLS

Los algoritmos que se AWS utilizan son un híbrido que combina la curva elíptica Diffie-Hellman (ECDH), un algoritmo clásico de intercambio de claves que se utiliza actualmente en el TLS, con Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), un algoritmo de cifrado y establecimiento de claves públicas que el Instituto Nacional de Estándares y Tecnología (NIST) ha designado como su primer algoritmo estándar de acuerdo de claves poscuántico. Este híbrido utiliza cada uno de los algoritmos de forma independiente para generar una clave. Luego combina las dos claves criptográficamente.

Obtenga más información sobre el PQC

Para obtener información sobre el proyecto de criptografía poscuántica del Instituto Nacional de Estándares y Tecnología (NIST), consulte Criptografía. Post-Quantum

Para obtener información sobre la estandarización de la criptografía poscuántica del NIST, consulte Estandarización de la criptografía. Post-Quantum

Habilitar el TLS poscuántico híbrido

Los SDK y las herramientas de AWS tienen capacidades y configuraciones criptográficas que difieren según el idioma y el tiempo de ejecución. Actualmente, un SDK o una herramienta de AWS proporcionan compatibilidad con PQ TLS de tres maneras:

Temas

- SDK con PQ TLS activado de forma predeterminada
- Opt-in Compatibilidad con PQ TLS
- SDK que se basan en el sistema OpenSSL
- Los SDK y las herramientas de AWS no tienen previsto admitir PQ TLS

SDK con PQ TLS activado de forma predeterminada

> **Note**
>
> A partir del 6Nov-2025, AWS SDK y sus bibliotecas CRT subyacentes para macOS y Windows utilizan bibliotecas del sistema para TLS, por lo que las capacidades de PQ TLS en esas plataformas suelen estar determinadas por el soporte a nivel de sistema.

AWS SDK para Go

El AWS SDK for Go utiliza la propia implementación de TLS de Golang proporcionada por su biblioteca estándar. Golang admite y prefiere PQ TLS a partir de la versión 1.24, por lo que los usuarios de AWS SDK for Go pueden habilitar PQ TLS simplemente actualizando Golang a la versión 1.24

AWS SDK para JavaScript (navegador)

El SDK de AWS para JavaScript (navegador) usa la pila de TLS del navegador, por lo que el SDK negociará el TLS de PQ si el motor de ejecución del navegador lo admite y lo prefiere. Firefox lanzó la compatibilidad con PQ TLS en la versión 132.0. Chrome anunció la compatibilidad con PQ TLS en la versión 1.3.1. Edge admite el protocolo PQ TLS opcional en la versión 120 para ordenadores de sobremesa y en la versión 140 para Android.

AWS SDK para Node.js

A partir de las versiones Node.js 22.20 (LTS) y 24.9.0, enlaza y agrupa OpenSSL 3.5 de Node.js forma estática. Esto significa que PQ TLS está activado y es el preferido de forma predeterminada para esas versiones y las posteriores.

SDK de AWS para Kotlin

El SDK de Kotlin admite y prefiere PQ TLS en Linux a partir de la versión 1.5.78. Como el CRT-based cliente de AWS SDK para Kotlin se basa en las bibliotecas del sistema para TLS en macOS y Windows, la compatibilidad con PQ TLS dependerá de las bibliotecas del sistema subyacentes.

SDK de AWS para Rust

El SDK de AWS para Rust distribuye paquetes distintos (conocidos como «cajas» en el ecosistema de Rust) para cada cliente de servicio. Todos ellos se administran en un GitHub repositorio consolidado, pero cada cliente de servicio sigue su propia cadencia de versiones y lanzamientos. El SDK consolidado publicó la preferencia de PQ TLS el 8/29 25 de diciembre, por lo que cualquier versión de un cliente de servicio individual que se publique después de esa fecha admitirá y preferirá PQ TLS de forma predeterminada.

Para determinar la versión mínima que admite PQ TLS para un cliente de servicio concreto, dirígete a la URL de la versión de crates.io correspondiente (por ejemplo, aquí encontrarás la de AWS Payment Cryptography) y buscando la primera versión publicada después del 29. Aug-25 Cualquier versión del cliente de servicio publicada después de la 29 tendrá el PQ TLS activado y Aug-25 será el preferido de forma predeterminada.

Opt-in Compatibilidad con PQ TLS

AWS SDK for C++

De forma predeterminada, el SDK de C++ usa clientes nativos de la plataforma, como libcurl y. WinHttp Libcurl generalmente se basa en el OpenSSL del sistema para TLS, por lo que el PQ TLS solo está habilitado de forma predeterminada si el OpenSSL del sistema es ≥ v3.5. Puedes anular esta configuración predeterminada en la versión 1.11.673 o posterior del SDK de C++ y optar por la versión que admite y habilita el PQ TLS de forma predeterminada. AwsCrtHttpClient

Notas sobre la creación para Opt-In PQ TLS Puedes recuperar las dependencias CRT del SDK con este script. La creación del SDK a partir del código fuente se describe aquí y aquí, pero ten en cuenta que es posible que necesites algunos indicadores CMake adicionales:

```
    -DUSE_CRT_HTTP_CLIENT=ON \
    -DUSE_TLS_V1_2=OFF \
    -DUSE_TLS_V1_3=ON \
    -DUSE_OPENSSL=OFF \
```

AWS SDK para Java

A partir de la versión 2, AWS SDK for Java proporciona un cliente HTTP AWS Common Runtime (AWS CRT) que se puede configurar para ejecutar PQ TLS. A partir de la versión 2.35.11, AwsCrtHttpClient habilita y prefiere el PQ TLS de forma predeterminada dondequiera que se utilice.

SDK que se basan en el sistema OpenSSL

Varios SDK y herramientas de AWS dependen de la libcrypto/libssl biblioteca del sistema para TLS. La biblioteca del sistema más utilizada es OpenSSL. OpenSSL habilitó la compatibilidad con PQ TLS en la versión 3.5, por lo que la forma más sencilla de configurar estos SDK y herramientas para PQ TLS es usarlos en una distribución de sistema operativo que tenga instalado al menos OpenSSL 3.5.

También puede configurar un contenedor Docker para que utilice OpenSSL 3.5 y habilite PQ TLS en cualquier sistema compatible con Docker. Consulte Post-quantum TLS en Python para ver un ejemplo de cómo configurarlo para Python.

CLI de AWS

La compatibilidad con PQ TLS con el instalador de AWS CLI estará disponible próximamente. Para habilitarlo inmediatamente, puede usar instaladores alternativos para la AWS CLI, que varía según el sistema operativo, y puede habilitar PQ TLS.

Para macOS, instale la AWS CLI a través de Homebrew y asegúrese de que su Homebrew-vended OpenSSL esté actualizado a la versión 3.5 o superior. Puede hacerlo con «brew install openssl @3 .6» y validarlo con «brew list | grep openssl».

Para Ubuntu o Debian Linux: asegúrese de que la distribución de Linux que está utilizando tenga instalado OpenSSL 3.5+ como sistema OpenSSL. A continuación, instale la AWS CLI mediante apt o PyPI. Con estos requisitos previos, la AWS CLI vendida por apt o PyPI se configurará para negociar. PQ-TLS Para obtener instrucciones paso a paso para validar la instalación, consulte el repositorio de GitHub y la entrada de blog adjunta.

AWS SDK para PHP

El AWS SDK for PHP se basa en el sistema libssl/libcrypto. Para usar PQ TLS, use este SDK en una distribución de sistema operativo que tenga instalado al menos OpenSSL 3.5.

AWS SDK para Python (Boto3)

El AWS SDK para Python (Boto3) se basa en el sistema. libssl/libcrypto Para usar PQ TLS, use este SDK en una distribución de sistema operativo que tenga instalado al menos OpenSSL 3.5.

AWS SDK para Ruby

El AWS SDK for Ruby se basa en el sistema libssl/libcrypto. Para usar PQ TLS, use este SDK en una distribución de sistema operativo que tenga instalado al menos OpenSSL 3.5.

AWS SDK para .NET

En Linux, AWS SDK for .NET se basa en el sistema libssl/libcrypto. Para usar PQ TLS, use este SDK en una distribución de sistema operativo que tenga instalado al menos OpenSSL 3.5. En Windows y macOS, PQ TLS está disponible a partir de .NET 10 y Windows 11. En macOS, la compatibilidad con TLS 1.3 (un requisito previo para PQ TLS) se puede habilitar al optar por Apple, como se describe aquí. Network.framework Suponiendo que la versión de .NET sea 10 como mínimo, PQ TLS debería estar habilitado.

Los SDK y las herramientas de AWS no tienen previsto admitir PQ TLS

Actualmente, no hay planes de admitir los siguientes SDK y herramientas lingüísticos:

- SDK de AWS para SAP
- SDK de AWS para Swift
- Herramientas de AWS para Windows PowerShell

Prácticas recomendadas de seguridad para la criptografía AWS de pagos

AWS La criptografía de pagos admite muchas funciones de seguridad integradas o que puede implementar de forma opcional para mejorar la protección de sus claves de cifrado y garantizar que se utilicen para los fines previstos, incluidas las políticas de IAM, un amplio conjunto de claves condicionales de políticas para refinar sus políticas de claves y políticas de IAM y la aplicación integrada de las normas PCI PIN en relación con los bloques de claves.

> **Important**
>
> Las directrices generales proporcionadas no representan una solución de seguridad completa. Dado que no todas las mejores prácticas son adecuadas para todas las situaciones, no se pretende que sean prescriptivas.

- Uso de claves y modos de uso: La criptografía de AWS pagos sigue y aplica las restricciones de uso y uso de claves tal como se describe en la especificación de bloque de claves de intercambio seguro de claves interoperable ANSI X9 TR 31-2018 y de conformidad con el requisito de seguridad 18-3 del PIN PCI. Esto limita la capacidad de utilizar una sola clave para varios fines y vincula criptográficamente los metadatos de la clave (como las operaciones permitidas) al propio material de la clave. AWS La criptografía de pagos impone automáticamente estas restricciones, por ejemplo, no se puede utilizar una clave de cifrado clave (TR31_K0_KEY_ENCRYPTION_KEY) para descifrar datos. Consulte Comprender los atributos clave de la clave AWS de criptografía de pagos para obtener más detalles.
- Limitar el uso compartido de material de clave simétrica: sólo comparta material de claves simétricas (como claves de cifrado de pines o claves de cifrado de claves) con un máximo de otra entidad. Si es necesario transferir material confidencial a más entidades o socios, cree claves adicionales. AWS La criptografía de pagos nunca expone el material de clave simétrica ni el material de clave privada asimétrica de forma transparente.
- Utilice alias o etiquetas para asociar las claves a determinados casos de uso o socios: los alias se pueden utilizar para indicar fácilmente el caso de uso asociado a una clave, por ejemplo, para indicar una clave de verificación de tarjeta asociada alias/BIN_12345_CVK al BIN 12345. Para ofrecer más flexibilidad, considere la posibilidad de crear etiquetas como bin=12345, use_case=acquiring,country=us,partner=foo. Los alias y las etiquetas también se pueden utilizar para limitar el acceso como, por ejemplo, para aplicar controles de acceso entre los casos de uso emisor y adquirente.
- Practicar el acceso con privilegio mínimo: IAM puede utilizarse para limitar el acceso de producción a los sistemas en lugar de a los individuos, como prohibir a los usuarios individuales la creación de claves o la ejecución de operaciones criptográficas. IAM también puede utilizarse para limitar el acceso tanto a comandos como a claves que pueden no ser aplicables para su caso de uso, como limitar la capacidad de generar o validar pines para un adquirente. Otra forma de utilizar el acceso con privilegio mínimo es restringir las operaciones sensibles (como la importación de claves) a cuentas de servicio específicas. Para ver ejemplos, consulte AWS Ejemplos de políticas de criptografía de pagos basadas en la identidad.

Véase también

- Gestión de identidad y acceso para criptografía AWS de pagos
- Consulte Prácticas recomendadas en IAM en la Guía del usuario de IAM.

Validación de conformidad para criptografía AWS de pagos

Al igual que con otros AWS servicios, los clientes requieren una comprensión clara del modelo de responsabilidad compartida en materia de seguridad y cumplimiento. Al tratarse de un servicio que admite pagos específicamente, es especialmente importante que los clientes de criptografía de AWS pagos comprendan el cumplimiento de las normas PCI aplicables. AWS Las evaluaciones de PCI DSS y PCI 3DS incluyen la criptografía de pagos. AWS Es posible que haya referencias al servicio en las guías de responsabilidad compartida, disponibles en, para estos informes. AWS Artifact Las evaluaciones de seguridad y Point-to-Point cifrado con PIN PCI (P2PE) son específicas de la criptografía de pagos. AWS

En esta sección se proporciona información sobre el estado y el alcance del cumplimiento del servicio, así como información que le será útil a la hora de planificar las evaluaciones de sus aplicaciones relacionadas con la seguridad de los códigos PCI PIN y PCI P2PE.

Temas

- Conformidad del servicio
- Planificación del cumplimiento de los PIN
- Uso del componente de descifrado de criptografía de AWS pagos en soluciones P2PE

Conformidad del servicio

Los auditores externos evalúan la seguridad y el cumplimiento de la criptografía de AWS pagos como parte de varios programas de AWS cumplimiento. Esto incluye SOC, PCI y otros.

AWS Además de los estándares PCI DSS y PCI 3DS, la criptografía de pagos se ha evaluado en relación con varios estándares PCI. Estos incluyen el cifrado PCI PIN Security (PCI PIN) y PCI (P2PE). Point-to-Point Consulte las certificaciones y las guías AWS Artifact de conformidad disponibles.

Para ver una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte Servicios de AWS incluidos . Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad en materia de cumplimiento al utilizar la criptografía de AWS pagos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar a garantizar el cumplimiento:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config :AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub CSPM—Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Planificación del cumplimiento de los PIN

Esta guía describe la documentación y las pruebas que necesitará para preparar una evaluación del PIN PCI de su aplicación de procesamiento de PIN que utilice criptografía de AWS pagos.

Al igual que ocurre con otras normas Servicios de AWS y normas de conformidad, es su responsabilidad utilizar el servicio de forma segura, configurando el control de acceso y utilizando los parámetros de seguridad de conformidad con los requisitos del PIN de PCI. En esta guía se analizarán esas configuraciones cuando sean adecuadas para cumplir un requisito.

Temas

- Temas comunes
- Alcance de la evaluación
- Operaciones de procesamiento de transacciones

Temas comunes

La migración de aplicaciones desde una conexión a HSM a un servicio gestionado, como la criptografía de AWS pagos, plantea problemas y conceptos comunes para los clientes y sus

asesores. En esta sección se proporciona información para aclarar cómo el uso seguro del servicio aborda estas situaciones.

Temas

- Responsabilidad compartida
- Configuración mínima de HSM
- Intercambio de claves entre el cliente y APC

Responsabilidad compartida

Los clientes que hayan asumido toda la responsabilidad en materia de seguridad y cumplimiento de las aplicaciones reestructurarán su conformidad para aprovechar la gestión de claves, los controles de seguridad y las capacidades gestionadas de HSM («el servicio») de AWS Payment Cryptography. Esto modificará por completo algunos requisitos AWS, como lo atestiguan las evaluaciones de terceros de AWS Payment Cryptography. Algunos requisitos se compartirán entre la solicitud del cliente y el servicio. Una aplicación es responsable de:

- Proporcionar información precisa al servicio
- Utilizar controles de seguridad de acuerdo con las recomendaciones del servicio y los requisitos de seguridad del PCI PIN
- Implementar los controles de seguridad necesarios mediante las herramientas proporcionadas por el servicio

Los clientes y sus asesores utilizarán las guías de responsabilidad compartida e implementación publicadas con las certificaciones de cumplimiento AWS Artifact para implementar los controles y la supervisión del control, y luego planificarán y completarán las evaluaciones.

Configuración mínima de HSM

El estándar de seguridad de datos PCI, el estándar fundamental de otros estándares PCI, exige que todos los sistemas estén configurados con la funcionalidad mínima necesaria para su funcionamiento. Los estándares PCI PIN, P2PE y otros estándares de soluciones aplican este requisito a la solución. HSMs HSMs debe habilitar únicamente las funciones necesarias para la solución.

AWS los servicios deben tratarse como sistemas y configurarse para ofrecer la funcionalidad mínima requerida. El estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) v4.0 de AWS

recomienda usar IAM para configurar la funcionalidad mínima de cada servicio de AWS que utilice la solución. Esto también se aplica a la criptografía de pagos. AWS Las políticas de IAM permiten permisos detallados para restringir las funciones criptográficas únicamente a los componentes de la aplicación que dependen de ellas.

Intercambio de claves entre el cliente y APC

PIN PIN Los requisitos de seguridad 8-4 y 15-2 exigen que el intercambio y la carga de las claves estén autenticadas y su integridad esté protegida. En el caso de la carga remota de los POI mediante claves, que se describe funcionalmente en el ANSI/ASC X9 TR-34 y se rige por el anexo A del PCI PIN, las claves públicas suelen figurar en certificados firmados por una autoridad de certificación que cumpla con el anexo A2. Para los intercambios entre organizaciones, las claves públicas utilizan otros mecanismos de autenticidad e integridad.

Todas las interacciones entre el cliente y AWS se realizan a través de AWS APIs, que autentica mutuamente cada llamada a la API y garantiza la integridad de las llamadas y las respuestas mediante TLS. AWS Identity and Access Management gestiona la autenticación de la aplicación del cliente con mecanismos como los tokens de seguridad y SigV4. El cliente autentica los puntos de enlace de la API de AWS mediante la autenticación del servidor TLS, que está integrada en AWS. SDKs Luego, TLS garantiza la confidencialidad e integridad de todos los datos que se transmiten entre el cliente y cada API de AWS.

APC APIs GetParametersForImport e ImportKey implementan una transferencia de claves del cliente al servicio. Si bien la autoridad de certificación (CA) proporcionada por GetParametersForImport ella no cumple con el anexo A2, es segura y exclusiva de la cuenta. Si bien no se puede confiar en que esta CA cumpla con los requisitos 8-4 y 15-2, sí que proporciona una verificación de integridad de la clave importada. También puede utilizar su propia CA aprovechando la API. GetCertificateSigningRequest

Los mecanismos que proporcionan autenticación de clave pública y garantía de integridad son:

- Autenticación proporcionada por la API de AWS
- La función MAC del certificado que proporciona proporciona la integridad de la clave GetParametersForImport, incluso si la información de identidad del certificado no es de confianza. La integridad de la clave también está asegurada por el MAC utilizado por TLS, protegiendo la sesión entre el cliente y AWS.

Los certificados y bloques de claves proporcionados por APC cumplen con el anexo A1, que especifica los requisitos para los certificados y la protección de claves mediante métodos asimétricos.

Alcance de la evaluación

El primer paso para planificar cualquier evaluación es documentar el alcance. En el caso del PCI PIN, el objetivo son los sistemas y procesos que protegen PINs, incluida la protección de las claves criptográficas y los dispositivos que las protegen: los terminales de pago, también denominados POI HSMs, y otros dispositivos criptográficos seguros points-of-interaction (SCD).

No abordaremos los requisitos sobre los que usted es plenamente responsable, ya que se refieren a áreas fuera del ámbito del servicio. Por ejemplo, la configuración y el aprovisionamiento de terminales de pago. Consulte la Guía de responsabilidad compartida sobre criptografía de AWS pagos para el PIN PCI, disponible en AWS Artifact

Temas

- Responsabilidad compartida
- Diagramas de red de nivel
- Tabla de claves
- Referencias de documentos

Responsabilidad compartida

AWS Payment Cryptography es una organización de cifrado y apoyo (ESO) y una entidad administradora externa (TPS) que adquiere PIN, según lo define el Programa de seguridad de PIN de Visa y figura en el Registro global de proveedores de servicios de Visa, bajo la denominación «Amazon Web Services, LLC». Esto significa que Visa permite que el servicio sea utilizado por un VisaNet procesador externo (VNP) que adquiere el PIN, un VisaNet procesador cliente que adquiere el PIN que actúa como proveedor de servicios y otros proveedores de TPS y ESO sin necesidad de una evaluación adicional por parte de los evaluadores de PIN del cliente (evaluadores de PIN calificados por PCI o PCI QPA).

Otras marcas de tarjetas o proveedores de redes de pago pueden confiar en el programa de seguridad de PIN de Visa o tener sus propios programas. Póngase en contacto con nosotros AWS Support si tiene preguntas sobre el cumplimiento de los servicios de otros programas de redes de pago.

AWS proporciona la certificación de conformidad (AOC) de seguridad (AOC) del PCI con PIN y la Guía de responsabilidad compartida para AWS la criptografía de pagos en. AWS Artifact El uso de proveedores de servicios en el procesamiento de los PIN es algo habitual desde hace muchos años; sin embargo, el estándar de seguridad PCI PIN, hasta la versión 3.1, no aborda la gestión de proveedores de servicios de terceros. Tampoco lo hace el programa de seguridad de PIN de Visa. Los clientes de QPA han seguido el modelo establecido en el PCI, el DSS, el AOC y la Guía de Responsabilidad Compartida, según el cual la prueba de AWS cumplimiento de los requisitos aplicables se considera satisfactoria.

Diagramas de red de nivel

La plantilla de informes de PIN PCI requiere: «En el caso de las entidades que se dedican al procesamiento de transacciones basadas en PIN, proporcione un esquema de red que describa los flujos de transacciones basadas en PIN con el uso del tipo de clave asociado. Además, KIFs las entidades que se dedican a la distribución remota de claves mediante técnicas asimétricas deberían proporcionar flujos de material de codificación»

AWS Payment Cryptography ha presentado la estructura interna del servicio para nuestra evaluación del PIN PCI. Sus diagramas ilustrarán cómo llamar al servicio APIs para procesar el PIN.

Ejemplo de diagrama de red de alto nivel para aplicaciones de PIN que utilizan criptografía AWS de pagos:

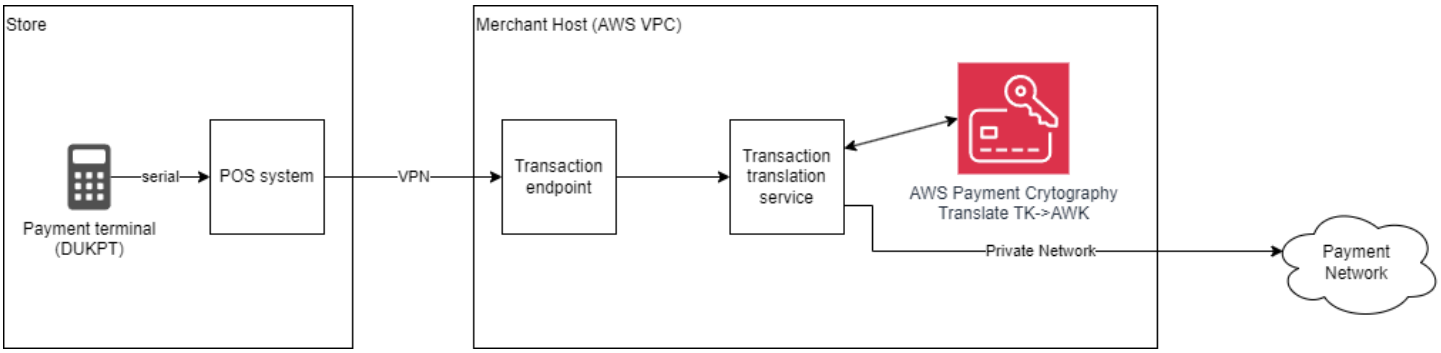


Tabla de claves

El informe exige que se enumeren todas las claves que protegen PINs, directa o indirectamente. Todas las claves que existan en el servicio se pueden incluir en la ListKeysAPI.

Asegúrese de proporcionar la lista de claves de todas las regiones y cuentas que poseen las claves de su aplicación.

Referencias de documentos

La documentación y las recomendaciones del proveedor para el uso seguro de la criptografía de AWS pagos se encuentran en la Guía del usuario y en la Referencia de la API. Estos están enlazados, según corresponda, en esta guía.

Operaciones de procesamiento de transacciones

Los requisitos del PIN PCI se organizan en los objetivos de control. Cada objetivo de control agrupa los requisitos para proteger un aspecto de la seguridad para PINs.

Temas

- Objetivo de control 1: los PINs utilizados en las transacciones regidas por estos requisitos se procesan utilizando equipos y metodologías que garantizan su seguridad.
- Objetivo de control 2: Las claves criptográficas utilizadas para la gestión del PIN encryption/decryption y las claves relacionadas se crean mediante procesos que garantizan que no sea posible predecir ninguna clave ni determinar si ciertas claves son más probables que otras.
- Objetivo de control 3: Las claves se transportan o transmiten de forma segura.
- Objetivo de control 4: La carga de claves en los HSMs dispositivos que aceptan el PIN del POI se gestiona de forma segura.
- Objetivo de control 5: Las claves se utilizan de forma que se evite o detecte su uso no autorizado.
- Objetivo de control 6: Las claves se administran de forma segura.
- Objetivo de control 7: El equipo utilizado para procesar PINs y gestionar las claves se gestiona de forma segura.

Objetivo de control 1: los PINs utilizados en las transacciones regidas por estos requisitos se procesan utilizando equipos y metodologías que garantizan su seguridad.

Requisito 1: los HSMs utilizados por AWS Payment Cryptography se evaluaron como parte de nuestra evaluación del PIN PCI. Para los clientes que utilizan el servicio, los requisitos 1 a 3 y 1 a 4 están «vigentes» en relación con el HSM gestionado por el servicio. Los resultados de HSM indicarán que las pruebas fueron certificadas por la QPA. AWS El certificado de conformidad con el PIN está disponible para consultarlo. AWS Artifact Será necesario inventariar y hacer referencia a otros SCD de su solución, como el POI.

Requisito 2: La documentación de sus procedimientos debe especificar cómo PINs se protege al titular de la tarjeta en lo que respecta a la divulgación a su personal, los protocolos de traducción del

PIN implementados y la protección durante el procesamiento en línea y fuera de línea. Además, la documentación debe contener un resumen de los métodos de administración de claves criptográficas utilizados en cada zona.

Requisito 3: El POI debe estar configurado para el cifrado y la transmisión seguros del PIN. AWS La criptografía de pagos solo admite las traducciones de bloques de PIN especificadas en el requisito 3-3.

Requisito 4: La aplicación no debe almacenar bloques de PIN. Los bloques de PIN, incluso cifrados, no deben conservarse en los diarios o registros de transacciones. El servicio no almacena los bloques de PIN y la evaluación de los PIN verifica que no estén en los registros.

Tenga en cuenta que el estándar de seguridad PCI PIN se aplica a la adquisición, «la gestión, el procesamiento y la transmisión seguros de los datos del número de identificación personal (PIN) durante el procesamiento de transacciones con tarjetas de pago en línea ATMs y fuera de línea en los terminales point-of-sale (POS)», tal como se indica en la norma. Sin embargo, el estándar se utiliza a menudo para evaluar la gestión de claves criptográficas para pagos que no están dentro del ámbito previsto. Esto puede incluir los casos de uso del emisor en los que PINs se almacenan. Las excepciones a los requisitos para estos casos deben acordarse con el público destinatario de la evaluación.

Objetivo de control 2: Las claves criptográficas utilizadas para la gestión del PIN encryption/decryption y las claves relacionadas se crean mediante procesos que garantizan que no sea posible predecir ninguna clave ni determinar si ciertas claves son más probables que otras.

Requisito 5: La generación de claves mediante criptografía de AWS pago se evaluó como parte de nuestra evaluación del PIN PCI. Esto se puede especificar en la columna «Generado por» de la tabla de claves.

Requisito 6: Los controles de seguridad de las claves contenidas en la criptografía de AWS pagos se evaluaron como parte de la evaluación del PIN PCI del servicio. Incluya descripciones de los controles de seguridad relacionados con la generación de claves en su aplicación y con cualquier otro proveedor de servicios.

Requisito 7: Debe tener una documentación sobre la política de generación de claves que especifique cómo se generan las claves y todas las partes afectadas deben conocer estos procedimientos o políticas. Los procedimientos para la creación de claves mediante la API de APC deben incluir el uso de funciones con permisos de creación de claves y aprobaciones para

ejecutar scripts u otro código que cree claves. AWS CloudTrail los registros contienen todos los CreateKeyeventos con fecha y hora, el ARN clave y los identificadores de usuario. Los números de serie y los registros de los HSM para acceder a los medios físicos se evaluaron como parte de la evaluación del PIN del servicio.

Objetivo de control 3: Las claves se transportan o transmiten de forma segura.

Requisito 8: La transferencia de claves mediante criptografía de AWS pago se evaluó como parte de nuestra evaluación del PIN PCI. Deberás documentar los mecanismos de protección clave de las transferencias antes de importarlas y después de exportarlas desde Payment Cryptography. AWS El servicio proporciona valores de verificación clave para todas las claves a fin de validar su correcta transferencia.

El requisito 8-4 exige que las claves públicas se transmitan de manera que se proteja su integridad y autenticidad. El intercambio entre su aplicación y AWS se controla mediante la autenticación de la aplicación y AWS, mediante AWS Identity and Access Management métodos, la autenticación de punto final de AWS la API a la aplicación mediante certificados de servidor TLS. Además, las claves públicas exportadas o importadas a AWS Payment Cryptography tienen certificados firmados por entidades efímeras específicas del cliente CAs (consulte, y). GetPublicKeyCertificateGetParametersForImportGetParametersForExport CAs No se pueden utilizar como único método de autenticación porque no cumplen con el anexo A2 de seguridad del PCI PIN. Sin embargo, los certificados siguen garantizando la integridad de las claves públicas, y IAM proporciona la autenticación.

Al intercambiar claves públicas con sus socios comerciales mediante métodos asimétricos, debe garantizar la autenticación de la empresa a través del canal de comunicación, mediante un sitio web seguro de intercambio de archivos, por ejemplo.

Requisito 9: El servicio no utiliza componentes clave de texto claro ni los admite directamente.

Requisito 10: El servicio impone la resistencia relativa de las llaves de protección para su transporte. Usted es responsable de transferir las claves antes de importarlas y después de exportarlas desde AWS Payment Cryptography y de utilizar los parámetros API y TR-31 que sean precisos para la importación, exportación y generación de claves. Debe disponer de procedimientos documentados para describir los mecanismos de transferencia de claves y la lista de claves criptográficas utilizadas para la transferencia.

Requisito 11: La documentación de sus procedimientos debe especificar cómo se transportan las llaves. Los procedimientos para la transferencia de claves mediante la API de criptografía de AWS

pagos deben incluir el uso de funciones con permisos de importación y exportación de claves y la aprobación de autorizaciones para ejecutar scripts u otro código que cree claves. AWS CloudTrail los registros contienen todos los eventos y. ImportKeyExportKey

Objetivo de control 4: La carga de claves en los HSMs dispositivos que aceptan el PIN del POI se gestiona de forma segura.

Requisito 12: Usted es responsable de cargar las claves de los componentes o recursos compartidos. La gestión de las claves principales del HSM se evaluó como parte de la evaluación del PIN del servicio. AWS La criptografía de pagos no carga claves de recursos compartidos o componentes individuales. Consulte la sección Detalles criptográficos.

Requisitos 13 y 14: Deberá describir la protección clave para las transferencias antes y después de la exportación desde el servicio.

Requisito 15: La criptografía de AWS pagos proporciona valores de verificación de claves para todas las claves del servicio y garantiza la integridad de las claves públicas. Su aplicación es responsable de utilizar estas comprobaciones para validar las claves después de importarlas o exportarlas desde el servicio. Debe documentar los procedimientos para asegurarse de que existe un mecanismo de validación.

El requisito 15-2 exige que las claves públicas se carguen de manera que se proteja su integridad y autenticidad. ImportKey, junto con GetParametersForImport, prevé la validación de los certificados de firma proporcionados. Si los certificados proporcionados son autofirmados, la autenticación debe proporcionarse mediante un mecanismo independiente, por ejemplo, el intercambio seguro de archivos.

Requisito 16: La documentación de sus procedimientos debe especificar cómo se cargan las claves en el servicio. Los procedimientos para la importación de claves mediante la API deben incluir el uso de funciones con permisos de importación de claves y aprobaciones para ejecutar scripts u otro código que cargue claves. AWS CloudTrail los registros contienen todos los ImportKeyeventos. Debe incluir los mecanismos de registro en la documentación. El servicio proporciona valores de comprobación clave para todas las claves a fin de validar la carga correcta de las claves.

Objetivo de control 5: Las claves se utilizan de forma que se evite o detecte su uso no autorizado.

Requisito 17: El servicio proporciona mecanismos, como etiquetas y alias, para las claves que permiten rastrear las relaciones de intercambio de claves. Además, los valores de verificación clave

deben mantenerse separados para demostrar que los valores clave conocidos o predeterminados no se utilizan cuando se comparten las claves.

Requisito 18: El servicio proporciona comprobaciones de integridad de las claves mediante GetKeyy ListKeysmediante eventos de gestión de claves AWS CloudTrail, mediante los cuales se pueden detectar sustituciones no autorizadas o supervisar la sincronización de las claves entre las partes. El servicio almacena las claves exclusivamente en bloques clave. Usted es responsable del almacenamiento y uso de las claves antes de importarlas y después de exportarlas desde AWS Payment Cryptography.

Debe disponer de procedimientos para una investigación inmediata en caso de que se produzca cualquier discrepancia durante el procesamiento de las transacciones basadas en un PIN o en caso de que se produzca algún imprevisto en la gestión de claves.

Requisito 19: El servicio utiliza las claves exclusivamente en los bloques clave, en la ejecución KeyUsage y en otros atributos clave para todas las operaciones. KeyModeOfUse Esto incluye la restricción de las operaciones con clave privada. Debe utilizar sus claves públicas para un único propósito, por ejemplo, el cifrado o la verificación de la firma digital, pero no para ambos. Debe utilizar cuentas separadas para la producción y test/development los sistemas.

Requisito 20: Usted es responsable de este requisito.

Objetivo de control 6: Las claves se administran de forma segura.

Requisito 21: El almacenamiento y el uso de las claves con criptografía de AWS pagos se evaluaron como parte de la evaluación del PIN PCI del servicio. En cuanto a los requisitos de almacenamiento relacionados con los componentes clave, usted es responsable de almacenarlos tal y como se describe en los puntos 21-2 y 21-3. Deberá describir los principales mecanismos de protección en la documentación de su política antes de la importación al servicio y después de su exportación desde el servicio.

Requisito 22: Los principales procedimientos de compromiso en materia de criptografía de AWS pagos se evaluaron como parte de la evaluación del PIN PCI del servicio. Deberá describir los principales procedimientos de detección y respuesta a las vulnerabilidades, incluidas la supervisión y la respuesta a las notificaciones emitidas por ellos. AWS

Requisito 23: La criptografía de AWS pagos no admite variantes ni otros métodos de cálculo de claves reversibles. Las claves principales de APC o las claves cifradas por ellas nunca están disponibles para los clientes. El uso del cálculo de claves reversibles se evaluó como parte de la evaluación del PIN PCI del servicio.

Requisito 24: Prácticas de destrucción de claves privadas y secretas internas La criptografía de AWS pagos se evaluó como parte de la evaluación del PIN PCI del servicio. Deberá describir el procedimiento de destrucción de claves antes de importarlas a APC y después de exportarlas desde APC. Los requisitos de destrucción relacionados con los componentes clave (24 y 24 horas y 23 horas) siguen siendo tu responsabilidad.

Requisito 25: El acceso a las claves secretas y privadas de la criptografía de AWS pagos se evaluó como parte de la evaluación del PIN PCI del servicio. Deberá disponer de un proceso y una documentación para controlar el acceso a las claves antes de importarlas y después de exportarlas desde AWS Payment Cryptography.

Requisito 26: Deberá describir el registro para acceder a las claves, los componentes clave o el material relacionado que se utilice fuera del servicio. Los registros de todas las actividades de administración clave que su aplicación realiza con el servicio están disponibles en AWS CloudTrail.

Requisito 27: Deberá describir los procedimientos de respaldo de las llaves, los componentes clave o el material relacionado que se utilice fuera del servicio.

Requisito 28: Los procedimientos para toda la administración de claves mediante la API deben incluir el uso de funciones con permisos de administración de claves y aprobaciones para ejecutar scripts u otro código que gestione las claves. AWS CloudTrail los registros contienen todos los eventos de administración clave

Objetivo de control 7: El equipo utilizado para procesar PINs y gestionar las claves se gestiona de forma segura.

Requisito 29: Sus requisitos de protección física y lógica HSMs se cumplen mediante el uso de la criptografía de AWS pagos.

Requisito 30: Su aplicación será responsable de todos los requisitos de protección física y lógica de los dispositivos POI.

Requisito 31: La protección de los dispositivos criptográficos seguros (SCD) utilizados por AWS Payment Cryptography se evaluó como parte de la evaluación del PIN PCI del servicio. Deberá demostrar la protección de cualquier otra aplicación SCDs utilizada por su aplicación.

Requisito 32: El uso de la criptografía SCDs utilizada en los AWS pagos se evaluó como parte de la evaluación del PIN PCI del servicio. Deberá demostrar el control de acceso y la protección de cualquier otra aplicación SCDs utilizada por su aplicación.

Requisito 33: Deberá describir las protecciones de cualquier equipo de procesamiento de PIN que esté bajo su control.

Uso del componente de descifrado de criptografía de AWS pagos en soluciones P2PE

Las soluciones PCI P2PE pueden utilizar el componente de descifrado de criptografía de pagos.AWS Esto se documenta en la sección Point-to-Point Cifrado PCI: requisitos de seguridad y procedimientos de prueba, soluciones P2PE y uso de terceros proveedores de componentes and/or P2PE: «Un proveedor de soluciones (o un comerciante como proveedor de soluciones) puede subcontratar ciertas funciones P2PE a proveedores de componentes P2PE que cotizan en PCI e informar el uso de los componentes P2PE listados en PCI en su informe de validación de P2PE (P-ROV)», que está disponible en el sitio web de PCI.

Al igual que con otros servicios y normas de conformidad de AWS, es su responsabilidad utilizar el servicio de forma segura, configurar el control de acceso y utilizar los parámetros de seguridad de acuerdo con los requisitos de PCI P2PE. La guía del usuario del componente de descifrado P2PE de criptografía de pagos de AWS, que está disponible en AWS Artifact, contiene instrucciones detalladas para integrar la criptografía de AWS pagos con su solución PCI P2PE y el informe anual del componente de descifrado, que es obligatorio para los informes de conformidad.

Gestión de identidad y acceso para criptografía AWS de pagos

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de criptografía de AWS pagos. La IAM es una herramienta Servicio de AWS que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona la criptografía de AWS pagos con IAM
- AWS Ejemplos de políticas de criptografía de pagos basadas en la identidad
- Resource-based políticas de criptografía de pagos AWS
- Multi-party aprobación de criptografía AWS de pagos
- Solución de problemas de identidad y acceso a la criptografía de AWS pagos

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de identidad y acceso a la criptografía de AWS pagos).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona la criptografía de AWS pagos con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte AWS Ejemplos de políticas de criptografía de pagos basadas en la identidad).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver la lista completa de las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios

pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud

cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona la criptografía de AWS pagos con IAM

Antes de utilizar IAM para gestionar el acceso a la criptografía de AWS pagos, debe saber qué funciones de IAM están disponibles para su uso con la criptografía de pagos. AWS Para obtener una visión general de cómo funcionan la criptografía de AWS pagos y otros AWS servicios con IAM, consulte AWS Servicios que funcionan con IAM en la Guía del usuario de IAM.

Temas

- AWS Políticas de criptografía de pagos Identity-based
- Autorización basada en etiquetas de criptografía de pago AWS

AWS Políticas de criptografía de pagos Identity-based

Con las políticas de IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. AWS La criptografía de pagos admite claves de condiciones, recursos y acciones específicas. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en criptografía de AWS pagos utilizan el siguiente prefijo antes de la acción:. `payment-cryptography:` Por ejemplo, para conceder a alguien permiso para ejecutar una operación de la API de `VerifyCardData` de AWS Payment Cryptography, incluya la acción `payment-cryptography:VerifyCardData` en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. AWS La criptografía de pagos define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "payment-cryptography:action1",
      "payment-cryptography:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List` (como, por ejemplo, `ListKeys` y `ListAliases`), incluya la siguiente acción:

```
"Action": "payment-cryptography:List*"
```

Para ver una lista de las acciones de criptografía de AWS pagos, consulte las acciones definidas por la criptografía de AWS pagos en la Guía del usuario de IAM.

Recursos

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

El recurso de clave de criptografía de pagos tiene el siguiente ARN:

```
arn:${Partition}:payment-cryptography:${Region}:${Account}:key/${keyARN}
```

Para obtener más información sobre el formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de AWS servicio.

Por ejemplo, para especificar la instancia de `arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h` en su instrucción, utilice el siguiente ARN:

```
"Resource": "arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h"
```

Para especificar todas las claves que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:payment-cryptography:us-east-2:111122223333:key/*"
```

Algunas acciones AWS de criptografía de pagos, como las de creación de claves, no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "*"
```

Para especificar varios recursos en una única instrucción, utilice una coma, tal y como se indica a continuación:

```
"Resource": [
      "resource1",
      "resource2"
```

Ejemplos

Para ver ejemplos de políticas de criptografía de AWS pagos basadas en la identidad, consulte. AWS Ejemplos de políticas de criptografía de pagos basadas en la identidad

Autorización basada en etiquetas de criptografía de pago AWS

Puede adjuntar etiquetas a los recursos AWS de criptografía de pagos o pasarlas en una solicitud a criptografía de AWS pagos. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `payment-cryptography:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

AWS Ejemplos de políticas de criptografía de pagos basadas en la identidad

De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear o modificar recursos de criptografía AWS de pagos. Tampoco pueden realizar tareas con la API Consola de

administración de AWS AWS CLI, o AWS . Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la consola de criptografía de pagos AWS
- Permitir a los usuarios consultar sus propios permisos
- Posibilidad de acceder a todos los aspectos de la criptografía de pagos AWS
- Posibilidad de llamar a las API mediante claves específicas
- Capacidad para denegar específicamente un recurso

Prácticas recomendadas relativas a políticas

Identity-based las políticas determinan si alguien puede crear recursos de criptografía de AWS pagos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de criptografía de pagos AWS

Para acceder a la consola de criptografía de AWS pagos, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de criptografía de AWS pagos de su AWS cuenta. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para garantizar que esas entidades puedan seguir utilizando la consola de criptografía de AWS pagos, adjunte también la siguiente política de AWS gestión a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Posibilidad de acceder a todos los aspectos de la criptografía de pagos AWS

> **Warning**
>
> Este ejemplo proporciona permisos amplios y no se recomienda. En su lugar, considere los modelos de acceso con menos privilegios.

En este ejemplo, desea conceder a un usuario de IAM de su AWS cuenta acceso a todas sus claves de criptografía de AWS pagos y la posibilidad de acceder a todas las API de criptografía de AWS pagos, incluidas ambas operaciones. `ControlPlane` `DataPlane`

JSON

```
{
      "Version":"2012-10-17",
      "Statement": [
            {
               "Effect": "Allow",
               "Action": [
                  "payment-cryptography:*"
               ],
               "Resource": [
                  "*"
               ]
            }
      ]
   }
```

Posibilidad de llamar a las API mediante claves específicas

En este ejemplo, quiere conceder a un usuario de IAM de su AWS cuenta acceso a una de sus claves de criptografía de AWS pagos y, a continuación, utilizar este recurso en dos API, `arn:aws:payment-cryptography:us-east-2:111122223333:key/kwapwa6qaifllw2h` y. `GenerateCardValidationData` `VerifyCardValidationData` Por el contrario, el usuario de IAM no tendrá acceso para usar esta clave en otras operaciones, como `DeleteKey` o `ExportKey`

Los recursos pueden ser claves con el prefijo `key` o alias con el prefijo `alias`.

JSON

```
   {
      "Version":"2012-10-17",
      "Statement": [
            {
               "Effect": "Allow",
               "Action": [
                  "payment-cryptography:VerifyCardValidationData",
                  "payment-cryptography:GenerateCardValidationData"
               ],
               "Resource": [
                  "arn:aws:payment-cryptography:us-east-2:111122223333:key/
kwapwa6qaifllw2h"
               ]
            }
      ]
   }
```

Capacidad para denegar específicamente un recurso

> **Warning**
>
> Considere detenidamente las implicaciones de conceder un acceso comodín. En su lugar, considere un modelo de privilegio mínimo.

En este ejemplo, quiere permitir que un usuario de IAM de su AWS cuenta acceda a cualquiera de sus claves de criptografía de AWS pagos, pero quiere denegar los permisos a una clave específica. El usuario tendrá acceso a `VerifyCardData` y `GenerateCardData` con todas las claves a excepción de la especificada en la instrucción de denegación.

JSON

```
{
```

```
      "Version":"2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "payment-cryptography:VerifyCardValidationData",
                  "payment-cryptography:GenerateCardValidationData"
              ],
              "Resource": [
                "arn:aws:payment-cryptography:us-east-2:111122223333:key/*"
              ]
          },
          {
              "Effect": "Deny",
              "Action": [
                "payment-cryptography:GenerateCardValidationData"
              ],
              "Resource": [
                "arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h"
              ]
          }
      ]
  }
```

Resource-based políticas de criptografía de pagos AWS

Resource-based las políticas son documentos de política de JSON que se adjuntan a un recurso, como una clave de criptografía de AWS pagos. En una política basada en recursos, se especifica quién puede acceder a la clave y las acciones que puede realizar en ella. Puede utilizar políticas basadas en recursos para:

- Conceda acceso a una sola clave a varios usuarios y roles.
- Conceda acceso a los usuarios o roles de otras AWS cuentas.

Temas

- Consideraciones
- Administrar las políticas basadas en los recursos
- Resource-based ejemplos de políticas

Al adjuntar una política basada en recursos a una clave de criptografía de AWS pagos, la criptografía de AWS pagos utiliza la lógica de evaluación de políticas de IAM para determinar si un mandante determinado está autorizado a realizar la acción solicitada. Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o entidades de IAM de otra cuenta como principal en una política basada en recursos. Cross-account el acceso requiere dos políticas:

1. Resource-based política (cuenta del propietario de la clave): el propietario de la clave utiliza `PutResourcePolicy` para conceder el acceso a la cuenta de la persona que llama o al director de IAM.
2. Identity-based política (cuenta de la persona que llama): el administrador de IAM de la persona que llama también debe permitir la acción de criptografía de AWS pagos (por ejemplo`payment-cryptography:EncryptData`) en la política de IAM de la persona que llama.

Ambas políticas deben permitir la acción. Si falta alguna de ellas, se deniega la solicitud de varias cuentas. `AccessDeniedException`

Si una política basada en los recursos permite el acceso a un principal de la misma cuenta, no se requiere ninguna política adicional basada en la identidad. Para obtener más información, consulte en qué se diferencian las funciones de IAM de Resource-based las políticas en la Guía del usuario de IAM.

⚠ Política de recursos: operaciones del plano de control

Resource-based las políticas no se aplican a las operaciones del plano de control de la política de recursos `PutResourcePolicy`, como `GetResourcePolicy`, y `DeleteResourcePolicy`. Esto evita posibles escenarios de bloqueo en los que una política de recursos pueda denegar la posibilidad de modificar o eliminar la propia política. El acceso a estas operaciones del plano de control se rige únicamente por las políticas de IAM basadas en la identidad.

Consideraciones

Tenga en cuenta lo siguiente cuando utilice políticas basadas en recursos con la criptografía de pagos. AWS

- AWS La criptografía de pagos impide automáticamente el acceso público a las claves. No puede crear una política basada en recursos que conceda acceso a directores públicos o anónimos. Todo

acceso a las claves AWS de criptografía de pagos requiere AWS directores autenticados, y el acceso público siempre está bloqueado.

- Resource-based las políticas se aplican por clave. Cada clave AWS de criptografía de pagos puede tener como máximo una política basada en recursos adjunta.
- Resource-based las políticas no se aplican a los alias. Cuando se hace referencia a una clave por su alias, se evalúa la política de recursos adjunta a la clave subyacente.
- Resource-based Las políticas no se aplican a las claves de región de réplica de solo lectura creadas mediante Multi-Region la replicación de claves en este momento. Las políticas de recursos solo se pueden adjuntar a la clave de región principal.
- El `Resource` elemento de una política basada en recursos debe ser `"*"` o coincidir exactamente con el ARN de la clave a la que se adjunta la política. Se `"*"` recomienda su uso porque permite reutilizar el mismo documento de política en varias claves.
- Las API de administración de políticas de recursos (`PutResourcePolicy``GetResourcePolicy`, y`DeleteResourcePolicy`) están restringidas al Cuenta de AWS propietario de la clave. Solo los directores de la cuenta del propietario de la clave pueden administrar las políticas de recursos.

Administrar las políticas basadas en los recursos

Puede administrar las políticas basadas en recursos para las claves de criptografía AWS de pagos mediante la API o. AWS CLI AWS Para usar este comando, sustituya el *`italicized placeholder text`* comando del ejemplo por su propia información.

Adjunte una política basada en recursos

Utilice la acción de la `PutResourcePolicy`API o el comando put-resource-policyCLI para adjuntar una política basada en recursos a una clave. Si ya existe una política, el comando la reemplaza.

En el siguiente ejemplo, se adjunta una política basada en recursos de un archivo JSON a una clave.

```
aws payment-cryptography put-resource-policy \
    --resource-arn arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h \
    --policy file://policy.json
```

Recupera una política basada en recursos

Utilice la acción de la `GetResourcePolicy`API o el comando get-resource-policyCLI para recuperar la política basada en recursos adjunta a una clave.

En el siguiente ejemplo, se recupera la política basada en recursos adjunta a una clave.

```
aws payment-cryptography get-resource-policy \
    --resource-arn arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h
```

La respuesta devuelve el documento de política:

```
{
    "Policy": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {
                    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
                },
                "Action": [
                    "payment-cryptography:EncryptData",
                    "payment-cryptography:DecryptData"
                ],
                "Resource": "*"
            }
        ]
    }
}
```

Eliminar una política basada en recursos

Utilice la acción de la DeleteResourcePolicyAPI o el comando delete-resource-policyCLI para eliminar la política basada en recursos de una clave.

En el siguiente ejemplo, se elimina la política basada en recursos adjunta a una clave.

```
aws payment-cryptography delete-resource-policy \
    --resource-arn arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h
```

Resource-based ejemplos de políticas

Otorgue acceso multicuenta a una clave

La siguiente política basada en los recursos concede a un usuario de otra AWS cuenta el permiso para utilizar una clave de criptografía de AWS pagos en operaciones criptográficas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
            },
            "Action": [
                "payment-cryptography:GenerateCardValidationData",
                "payment-cryptography:VerifyCardValidationData"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorga diferentes permisos a diferentes cuentas

La siguiente política basada en los recursos demuestra cómo conceder distintos permisos a los directores de cuentas distintas. En este ejemplo, un servidor de control de acceso (ACS) de una cuenta puede generar datos de validación de tarjetas, mientras que un servicio de autorización de pago de una cuenta diferente solo puede validar criptogramas de 3DS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow3DSACSToGenerate",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/3dsAcsRole"
            },
            "Action": [
```

```
                "payment-cryptography:GenerateCardValidationData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowPaymentAuthToVerify",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:role/PaymentAuthRole"
            },
            "Action": [
                "payment-cryptography:VerifyAuthRequestCryptogram"
            ],
            "Resource": "*"
        }
    ]
}
```

Multi-party aprobación de criptografía AWS de pagos

AWS La criptografía de pagos se integra con Multi-party la aprobación (MPA), una capacidad de Amazon Web Services Organizations, para ayudar a proteger las operaciones críticas mediante un proceso de aprobación distribuido. Con la MPA, puede exigir que varias personas de confianza aprueben determinadas operaciones de criptografía de AWS pagos antes de llevarlas a cabo.

Temas

- Descripción general de
- Operaciones protegidas
- Requisitos previos
- Activación y desactivación de la MPA
- Introducción
- Ejemplo: importe un certificado raíz con la MPA habilitada
- AWS CloudTrail registro de eventos de MPA
- Comprobar el estado de las solicitudes y gestionar los errores

Descripción general de

Multi-party La aprobación añade un nivel adicional de seguridad a las operaciones confidenciales de criptografía de AWS pagos, ya que requiere la aprobación de un grupo de personas de confianza antes de que la operación pueda continuar. Esto ayuda a proteger contra los cambios no autorizados en caso de que un único conjunto de credenciales se vea comprometido e impide que una sola persona realice un cambio unilateral.

Un equipo de aprobación es un grupo de aprobadores de su organización que usted designa para aprobar o denegar las solicitudes de operaciones protegidas. Los aprobadores de su organización gestionan en su totalidad el proceso de aprobación. Ningún miembro AWS del personal participa en la aprobación o denegación de las solicitudes.

Cuando el MPA está activado para una operación protegida, ocurre lo siguiente:

1. Un solicitante inicia la operación protegida.
2. La MPA crea una sesión de aprobación y notifica a los miembros del equipo de aprobación.
3. Los miembros del equipo de aprobación revisan la solicitud y la aprueban o rechazan a través del portal de la MPA.
4. Una vez que se alcanza el umbral mínimo de aprobaciones requerido, la operación continúa. Si el equipo de aprobación rechaza la solicitud o si el tiempo de sesión permitido expira antes de alcanzar el umbral de aprobación, la operación no se lleva a cabo. En ambos casos, el solicitante debe enviar una nueva solicitud para volver a intentar la operación.

> **Note**
>
> Al importar un certificado de CA raíz con el MPA activado, el `RequesterComment` parámetro es obligatorio. Este comentario se incluye en la notificación de aprobación que se envía al equipo de aprobación y proporciona el contexto de la solicitud.

Operaciones protegidas

AWS La criptografía de pagos admite la MPA para las siguientes operaciones:

- `ImportKey`con material `RootCertificatePublicKey` clave: la importación de un certificado de clave pública raíz es una operación fundamental, ya que los certificados raíz establecen la

base de confianza para todas las importaciones y exportaciones de claves posteriores mediante un intercambio de claves asimétrico, como. TR-34 Exigir la aprobación de varias partes para esta operación ayuda a garantizar que ninguna persona pueda establecer o cambiar unilateralmente la raíz de confianza de sus claves de criptografía de AWS pagos.

Requisitos previos

Antes de poder utilizar la MPA con la criptografía AWS de pagos, debe cumplir los siguientes requisitos previos:

- Configure MPA en su entorno de Amazon Web Services Organizations. Para obtener instrucciones, consulte ¿Qué es Multi-party la aprobación? en la Guía del usuario de Multi-party aprobación.
- Cree al menos un equipo de aprobación con los aprobadores necesarios.
- Comparta el equipo de aprobación con el equipo Cuenta de AWS que contiene sus claves AWS de criptografía de pago. AWS Resource Access Manager
- La cuenta de administración de su organización debe estar habilitada para su Multi-party aprobación.

Activación y desactivación de la MPA

Una vez que haya creado un equipo de aprobación, podrá habilitar la MPA para la criptografía de AWS pagos asociando el equipo a su cuenta. También puede deshabilitar el MPA desasociando el equipo, aunque la desasociación requiere la aprobación del equipo de aprobación actualmente asociado.

Habilite el MPA

Utilice la acción de la `AssociateMpaTeam` API o el comando associate-mpa-team CLI para asociar un equipo de aprobación a su cuenta de criptografía de AWS pagos. Una vez asociadas, las operaciones protegidas requieren la aprobación del equipo para poder continuar.

```
aws payment-cryptography associate-mpa-team \
    --team-arn arn:aws:mpa:us-east-1:111122223333:team/my-approval-team
```

Desactivar el MPA

Utilice la acción de la `DisassociateMpaTeam` API o el comando disassociate-mpa-team CLI para eliminar la asociación del equipo de aprobación. La disociación de un equipo es en sí misma una operación protegida que requiere la aprobación del equipo de aprobación actualmente asociado.

```
aws payment-cryptography disassociate-mpa-team \
    --team-arn arn:aws:mpa:us-east-1:111122223333:team/my-approval-team
```

Important

La desactivación del MPA requiere la aprobación del equipo de aprobación actualmente asociado. Esto garantiza que ninguna persona pueda eliminar unilateralmente la protección de aprobación multipartidista.

Note

El `--requester-comment` parámetro es opcional para associate-mpa-team y. disassociate-mpa-team

Introducción

Para empezar a utilizar la MPA para la criptografía de AWS pagos, consulte la Guía del usuario de Multi-party aprobación para obtener instrucciones de configuración detalladas, que incluyen cómo crear equipos de aprobación, configurar las políticas de aprobación y gestionar las sesiones de aprobación.

Ejemplo: importe un certificado raíz con la MPA habilitada

Una vez que se habilita el MPA y se asocia un equipo de aprobación a la `ImportKey` operación`RootCertificatePublicKey`, la solicitud de importación debe aprobarse antes de continuar.

1. Un solicitante llama `import-key` para importar un certificado de clave pública raíz. Para usar este comando, sustituya *`italicized placeholder text`* el comando del ejemplo por su propia información.

   ```
   aws payment-cryptography import-key \
   ```

```
    --key-material='{"RootCertificatePublicKey": {
    "KeyAttributes": {
        "KeyAlgorithm": "RSA_4096",
        "KeyClass": "PUBLIC_KEY",
        "KeyModesOfUse": {"Verify": true},
        "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE"
    },
    "PublicKeyCertificate": "LS0tLS1CRUdJTi..."}}' \
    --requester-comment "Importing new root CA certificate for TR-34 key exchange
 with partner XYZ"
```

La respuesta devuelve una clave `KeyState` establecida en`CREATE_IN_PROGRESS`, lo que indica que la solicitud está pendiente de aprobación. La respuesta también incluye `MpaStatus` detalles sobre la sesión de aprobación:

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE",
            "KeyClass": "PUBLIC_KEY",
            "KeyAlgorithm": "RSA_4096"
        },
        "Enabled": true,
        "KeyState": "CREATE_IN_PROGRESS",
        "KeyOrigin": "EXTERNAL",
        "CreateTimestamp": "2026-04-27T10:15:30.000000+00:00",
        "UsageStartTimestamp": "2026-04-27T10:15:29.926000+00:00",
        "MpaStatus": {
            "MpaSessionArn": "arn:aws:mpa:us-
east-1:111122223333:session/abc123def456",
            "Status": "PENDING",
            "InitiationDate": "2026-04-27T10:15:30.000000+00:00"
        }
    }
}
```

2. Como la MPA está habilitada, la solicitud no se completa de forma inmediata. En su lugar, AWS Payment Cryptography crea una sesión de aprobación y devuelve una respuesta que indica que la aprobación está pendiente.

3. Los miembros del equipo de aprobación reciben una notificación y revisan la solicitud a través del portal de la MPA. Una vez que el número requerido de aprobadores apruebe la solicitud, la operación de importación continúa y se importa el certificado raíz.

AWS CloudTrail registro de eventos de MPA

Cuando la MPA está habilitada, la criptografía de AWS pagos registra los eventos del servicio hasta que AWS CloudTrailfinaliza una sesión de aprobación. Estos eventos registran el resultado del proceso de aprobación, incluso si la solicitud se aprobó o no. Puede utilizar estos registros para auditar la actividad de la MPA y realizar un seguimiento del estado de las operaciones protegidas.

MPA-related CloudTrail los eventos incluyen los siguientes campos en`serviceEventDetails`:

- `keyArn`— El ARN de la clave afectada por la operación.
- `operation`— La operación protegida que se solicitó.
- `mpaSessionArn`— El ARN de la sesión de aprobación de la MPA.
- `sessionStatus`— El resultado de la sesión de aprobación (`APPROVEDoFAILED`).

Solicitud aprobada

El siguiente ejemplo muestra un CloudTrail evento para una `ImportKey` solicitud que fue aprobada por el equipo de la MPA:


```
{
    "eventVersion": "1.11",
    "eventTime": "2026-04-28T18:49:51Z",
    "eventName": "ImportKey",
    "eventSource": "payment-cryptography.amazonaws.com",
    "eventType": "AwsServiceEvent",
    "eventCategory": "Management",
    "awsRegion": "us-east-1",
    "readOnly": false,
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "payment-cryptography.amazonaws.com"
    },
    "resources": [
```

```
        {
            "ARN": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/spa2dclzmsihlj4o",
            "accountId": "111122223333",
            "type": "AWS::PaymentCryptography::Key"
        }
    ],
    "serviceEventDetails": {
        "keyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/spa2dclzmsihlj4o",
        "operation": "ImportKey",
        "mpaSessionArn": "arn:aws:mpa:us-east-1:111122223333:session/my-approval-
team/44c76e07-8937-4d7d-bb9a-a646322e2a1e",
        "sessionStatus": "APPROVED"
    }
}
```

Solicitud fallida

En el siguiente ejemplo, se muestra un CloudTrail evento de una `ImportKey` solicitud que se denegó o se agotó el tiempo de espera:

```
{
    "eventVersion": "1.11",
    "eventTime": "2026-04-28T18:50:35Z",
    "eventName": "ImportKey",
    "eventSource": "payment-cryptography.amazonaws.com",
    "eventType": "AwsServiceEvent",
    "eventCategory": "Management",
    "awsRegion": "us-east-1",
    "readOnly": false,
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "payment-cryptography.amazonaws.com"
    },
    "resources": [
        {
            "ARN": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/qj46ku4qimypxdo7",
            "accountId": "111122223333",
            "type": "AWS::PaymentCryptography::Key"
```

```
        }
    ],
    "serviceEventDetails": {
        "keyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/qj46ku4qimypxdo7",
        "operation": "ImportKey",
        "mpaSessionArn": "arn:aws:mpa:us-east-1:111122223333:session/my-approval-team/
b0ac1994-14e1-47a6-bf1a-0b6fc0b845f2",
        "sessionStatus": "FAILED"
    }
}
```

Para obtener más información AWS CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Comprobar el estado de las solicitudes y gestionar los errores

Puede comprobar el estado de una solicitud de MPA pendiente llamando `GetKey`. La respuesta incluye el `MpaStatus` campo con los detalles de la sesión de aprobación actual. Para usar este comando, sustituya *`italicized placeholder text`* el comando del ejemplo por su propia información.

```
aws payment-cryptography get-key \
    --key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h
```

Mientras la solicitud esté pendiente de aprobación, la respuesta se mostrará `KeyState` como `CREATE_IN_PROGRESS` y `MpaStatus.Status` como`PENDING`:

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE",
            "KeyClass": "PUBLIC_KEY",
            "KeyAlgorithm": "RSA_4096"
        },
        "Enabled": true,
        "KeyState": "CREATE_IN_PROGRESS",
        "KeyOrigin": "EXTERNAL",
        "CreateTimestamp": "2026-04-27T10:15:30.000000+00:00",
        "UsageStartTimestamp": "2026-04-27T10:15:29.926000+00:00",
```

```
        "MpaStatus": {
            "MpaSessionArn": "arn:aws:mpa:us-east-1:111122223333:session/abc123def456",
            "Status": "PENDING",
            "InitiationDate": "2026-04-27T10:15:30.000000+00:00"
        }
    }
}
```

Una vez que el número requerido de aprobadores apruebe la solicitud, `KeyState` se mueve a `CREATE_COMPLETE` y `MpaStatus.Status` a`APPROVED`. La clave ya está lista para su uso:

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE",
            "KeyClass": "PUBLIC_KEY",
            "KeyAlgorithm": "RSA_4096"
        },
        "Enabled": true,
        "KeyState": "CREATE_COMPLETE",
        "KeyOrigin": "EXTERNAL",
        "CreateTimestamp": "2026-04-27T10:15:30.000000+00:00",
        "UsageStartTimestamp": "2026-04-27T10:15:29.926000+00:00",
        "MpaStatus": {
            "MpaSessionArn": "arn:aws:mpa:us-east-1:111122223333:session/abc123def456",
            "Status": "APPROVED",
            "InitiationDate": "2026-04-27T10:15:30.000000+00:00"
        }
    }
}
```

Si el equipo de aprobación rechaza la solicitud o la sesión caduca antes de que se alcance el umbral de aprobación, `KeyState` cambia `CREATE_FAILED` y `MpaStatus.Status` cambia a`FAILED`:

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_S0_ASYMMETRIC_KEY_FOR_DIGITAL_SIGNATURE",
```

```
            "KeyClass": "PUBLIC_KEY",
            "KeyAlgorithm": "RSA_4096"
        },
        "Enabled": true,
        "KeyState": "CREATE_FAILED",
        "KeyOrigin": "EXTERNAL",
        "CreateTimestamp": "2026-04-27T10:15:30.000000+00:00",
        "UsageStartTimestamp": "2026-04-27T10:15:29.926000+00:00",
        "MpaStatus": {
            "MpaSessionArn": "arn:aws:mpa:us-east-1:111122223333:session/abc123def456",
            "Status": "FAILED",
            "InitiationDate": "2026-04-27T10:15:30.000000+00:00",
            "StatusMessage": "Approval session expired or was denied"
        }
    }
}
```


No se puede usar una clave en `CREATE_FAILED` estado para operaciones criptográficas. Para volver a intentar la importación, debe enviar una nueva `ImportKey` solicitud, que creará una nueva sesión de aprobación.

Solución de problemas de identidad y acceso a la criptografía de AWS pagos

Se añadirán temas a esta sección a medida que se IAM-related identifiquen problemas específicos de la criptografía de AWS pagos. Para obtener información general sobre la solución de problemas relacionados con la IAM, consulte la sección de solución de problemas de la Guía del usuario de IAM.

Supervisión de la criptografía AWS de pagos

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de la criptografía de AWS pagos y del resto de las soluciones de AWS. AWS proporciona las siguientes herramientas de supervisión para controlar la criptografía de AWS pagos, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puedes CloudWatch hacer un seguimiento del uso de algunos APIs o notificarte si te estás acercando a tus cuotas de criptografía de AWS pagos. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde EC2 instancias de Amazon y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcanzan ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, el punto final al que se llamó, los recursos (claves) utilizados, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte la AWS CloudTrail Guía del usuario de .

Temas

- Registro de llamadas a la API de criptografía de AWS pagos mediante AWS CloudTrail

Registro de llamadas a la API de criptografía de AWS pagos mediante AWS CloudTrail

AWS La criptografía de pagos está integrada con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en criptografía de AWS pagos. CloudTrail captura todas las llamadas a la API para la criptografía AWS de pagos como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de y las llamadas desde el código a las operaciones de la API de . Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de criptografía de AWS pagos. Si no configura un registro, podrá ver los eventos de administración (plano de control) más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar la solicitud que se realizó a AWS Payment Cryptography, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Temas

- AWS Información sobre criptografía de pagos en CloudTrail
- Controle los eventos del plano en CloudTrail
- Eventos de datos en CloudTrail
- Comprensión AWS de las entradas de los archivos de registro del plano de control de criptografía de pagos
- Descripción de las entradas de los archivos de registro del plano de datos de criptografía de AWS pagos

AWS Información sobre criptografía de pagos en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en la criptografía de AWS pagos, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Se puede ver, buscar y descargar los últimos eventos de la cuenta de AWS . Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los relacionados con la criptografía de AWS pagos, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de

seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS . La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones
- Recibir archivos de CloudTrail registro de varias cuentas

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Controle los eventos del plano en CloudTrail

CloudTrail registra las operaciones de criptografía de AWS pagos, como CreateKey,, ImportKeyDeleteKeyListKeysTagResource, y todas las demás operaciones del plano de control.

Eventos de datos en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos que se realizan en un recurso o dentro de él, como el cifrado de una carga útil o la traducción de un PIN. Los eventos de datos son actividades de gran volumen que CloudTrail no se registran de forma predeterminada. Puede habilitar el registro de acciones de la API de eventos de datos para los eventos del plano de datos de criptografía de AWS pagos mediante nuestra consola CloudTrail APIs . Para obtener más información, consulte Registro de eventos de datos en la Guía del usuario de AWS CloudTrail .

Con CloudTrail, debe utilizar selectores de eventos avanzados para decidir qué actividades de la API de criptografía de AWS pagos se registran y registran. Para registrar los eventos del plano de datos de criptografía de AWS pagos, debes incluir el tipo de recurso y. `AWS Payment Cryptography key` `AWS Payment Cryptography alias` Una vez establecido esto, puede ajustar aún más las preferencias de registro seleccionando eventos de datos específicos para registrarlos, por ejemplo, mediante el uso del filtro `eventName` para realizar un seguimiento de los eventos de `EncryptData`. Para obtener más información, consulta `AdvancedEventSelector` en la AWS CloudTrail Referencia de la API de .

> **Note**
>
> Para suscribirse a los eventos de datos de criptografía de AWS pagos, debe utilizar selectores de eventos avanzados. Recomendamos suscribirse a los eventos clave y de alias para asegurarse de recibir todos los eventos.

AWS Eventos de datos de criptografía de pagos:

- `DecryptData`
- `EncryptData`
- `GenerateCardValidationData`
- `GenerateMac`
- `GeneratePinData`
- `ReEncryptData`
- `TranslatePinData`
- `VerifyAuthRequestCryptogram`
- `VerifyCardValidationData`
- `VerifyMac`
- `VerifyPinData`

Se aplican cargos adicionales a los eventos de datos. Para obtener más información, consulte AWS CloudTrail Precios.

Comprensión AWS de las entradas de los archivos de registro del plano de control de criptografía de pagos

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra la `CreateKey` acción AWS de criptografía de pagos.

```
      {
    CloudTrailEvent: {
      tlsDetails= {
        TlsDetails: {
          cipherSuite=TLS_AES_128_GCM_SHA256,
          tlsVersion=TLSv1.3,
          clientProvidedHostHeader=controlplane.paymentcryptography.us-
west-2.amazonaws.com
        }
      },
    requestParameters=CreateKeyInput (
      keyAttributes=KeyAttributes(
        KeyUsage=TR31_B0_BASE_DERIVATION_KEY,
        keyClass=SYMMETRIC_KEY,
        keyAlgorithm=AES_128,
        keyModesOfUse=KeyModesOfUse(
          encrypt=false,
          decrypt=false,
          wrap=false
          unwrap=false,
          generate=false,
          sign=false,
          verify=false,
          deriveKey=true,
          noRestrictions=false)
        ),
      keyCheckValueAlgorithm=null,
      exportable=true,
```

```
      enabled=true,
      tags=null),
    eventName=CreateKey,
    userAgent=Coral/Apache-HttpClient5,
    responseElements=CreateKeyOutput(
      key=Key(
        keyArn=arn:aws:payment-cryptography:us-
east-2:111122223333:key/5rplquuwozodpwsp,
          keyAttributes=KeyAttributes(
            KeyUsage=TR31_B0_BASE_DERIVATION_KEY,
            keyClass=SYMMETRIC_KEY,
            keyAlgorithm=AES_128,
            keyModesOfUse=KeyModesOfUse(
              encrypt=false,
              decrypt=false,
              wrap=false,
              unwrap=false,
              generate=false,
              sign=false,
              verify=false,
              deriveKey=true,
              noRestrictions=false)
            ),
          keyCheckValue=FE23D3,
          keyCheckValueAlgorithm=ANSI_X9_24,
          enabled=true,
          exportable=true,
          keyState=CREATE_COMPLETE,
          keyOrigin=AWS_PAYMENT_CRYPTOGRAPHY,
          createTimestamp=Sun May 21 18:58:32 UTC 2023,
          usageStartTimestamp=Sun May 21 18:58:32 UTC 2023,
          usageStopTimestamp=null,
          deletePendingTimestamp=null,
          deleteTimestamp=null)
        ),
      sourceIPAddress=192.158.1.38,
        userIdentity={
          UserIdentity: {
            arn=arn:aws:sts::111122223333:assumed-role/TestAssumeRole-us-west-2/
ControlPlane-IntegTest-68211a2a-3e9d-42b7-86ac-c682520e0410,
            invokedBy=null,
            accessKeyId=TESTXECZ5U2ZULLHHMJG,
            type=AssumedRole,
            sessionContext={
```

```
              SessionContext: {
                sessionIssuer={
                  SessionIssuer: {arn=arn:aws:iam::111122223333:role/TestAssumeRole-us-
west-2,
                  type=Role,
                  accountId=111122223333,
                  userName=TestAssumeRole-us-west-2,
                  principalId=TESTXECZ5U9M4LGF2N6Y5}
                },
                attributes={
                  SessionContextAttributes: {
                    creationDate=Sun May 21 18:58:31 UTC 2023,
                    mfaAuthenticated=false
                  }
                },
                webIdFederationData=null
              }
            },
          username=null,
          principalId=TESTXECZ5U9M4LGF2N6Y5:ControlPlane-User,
          accountId=111122223333,
          identityProvider=null
        }
      },
      eventTime=Sun May 21 18:58:32 UTC 2023,
      managementEvent=true,
      recipientAccountId=111122223333,
      awsRegion=us-west-2,
      requestID=151cdd67-4321-1234-9999-dce10d45c92e,
      eventVersion=1.08, eventType=AwsApiCall,
      readOnly=false,
      eventID=c69e3101-eac2-1b4d-b942-019919ad2faf,
      eventSource=payment-cryptography.amazonaws.com,
      eventCategory=Management,
      additionalEventData={
    }
  }
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra que la criptografía de AWS pagos permite la replicación de claves multirregionales.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "payment-cryptography.amazonaws.com"
    },
    "eventTime": "2025-08-15T17:50:41Z",
    "eventSource": "payment-cryptography.amazonaws.com",
    "eventName": "SynchronizeMultiRegionKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "payment-cryptography.amazonaws.com",
    "userAgent": "payment-cryptography.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "55c0fcbc-5b2e-4bd2-a976-99305be6e6fc",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "keyArn": "arn:aws:payment-cryptography:us-east-1:111122223333:key/key-id",
        "replicationRegion": "us-east-2"
    },
    "eventCategory": "Management"
}
```


Descripción de las entradas de los archivos de registro del plano de datos de criptografía de AWS pagos

Los eventos del plano de datos se pueden configurar opcionalmente y funcionan de manera similar a los registros del plano de control, pero suelen tener volúmenes mucho más altos. Dado el carácter confidencial de algunas entradas y salidas de las operaciones del plano de datos de criptografía de AWS pagos, es posible que en algunos campos aparezca el mensaje «*** Datos confidenciales redactados ***». Esto no se puede configurar y su objetivo es evitar que los datos confidenciales aparezcan en los registros o registros.

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra la `EncryptData` acción de criptografía de AWS pagos.


```
    {
```

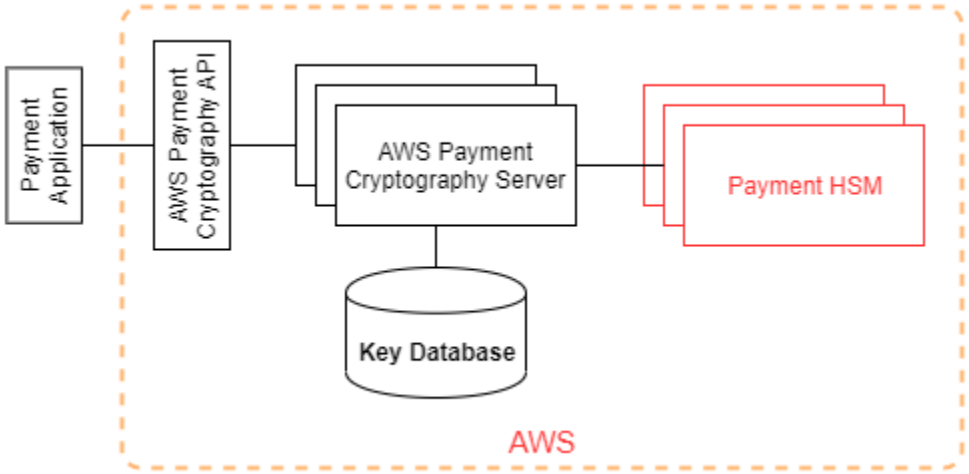
```
        "Records": [
            {
                "eventVersion": "1.09",
                "userIdentity": {
                    "type": "AssumedRole",
                    "principalId": "TESTXECZ5U2ZULLHHMJG:DataPlane-User",
                    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/DataPlane-
User",
                    "accountId": "111122223333",
                    "accessKeyId": "TESTXECZ5U2ZULLHHMJG",
                    "userName": "",
                    "sessionContext": {
                        "sessionIssuer": {
                            "type": "Role",
                            "principalId": "TESTXECZ5U9M4LGF2N6Y5",
                            "arn": "arn:aws:iam::111122223333:role/Admin",
                            "accountId": "111122223333",
                            "userName": "Admin"
                        },
                        "attributes": {
                            "creationDate": "2024-07-09T14:23:05Z",
                            "mfaAuthenticated": "false"
                        }
                    }
                },
                "eventTime": "2024-07-09T14:24:02Z",
                "eventSource": "payment-cryptography.amazonaws.com",
                "eventName": "GenerateCardValidationData",
                "awsRegion": "us-east-2",
                "sourceIPAddress": "192.158.1.38",
                "userAgent": "aws-cli/2.17.6 md/awscrt#0.20.11 ua/2.0 os/macos#23.4.0
 md/arch#x86_64 lang/python#3.11.8 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#payment-cryptography-data.generate-card-
validation-data",
                "requestParameters": {
                    "key_identifier": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/5rplquuwozodpwsp",
                    "primary_account_number": "*** Sensitive Data Redacted ***",
                    "generation_attributes": {
                        "CardVerificationValue2": {
                            "card_expiry_date": "*** Sensitive Data Redacted ***"
                        }
                    }
                },
```

```
                "responseElements": null,
                "requestID": "f2a99da8-91e2-47a9-b9d2-1706e733991e",
                "eventID": "e4eb3785-ac6a-4589-97a1-babdd3d4dd95",
                "readOnly": true,
                "resources": [
                    {
                        "accountId": "111122223333",
                        "type": "AWS::PaymentCryptography::Key",
                        "ARN": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/5rplquuwozodpwsp"
                    }
                ],
                "eventType": "AwsApiCall",
                "managementEvent": false,
                "recipientAccountId": "111122223333",
                "eventCategory": "Data",
                "tlsDetails": {
                    "tlsVersion": "TLSv1.3",
                    "cipherSuite": "TLS_AES_128_GCM_SHA256",
                    "clientProvidedHostHeader": "dataplane.payment-cryptography.us-
east-2.amazonaws.com"
                }
            }
        ]
    }
```

Detalles criptográficos

AWS La criptografía de pagos proporciona una interfaz web para generar y administrar claves criptográficas para las transacciones de pago. AWS La criptografía de pagos ofrece servicios estándar de administración de claves y herramientas y criptografía de transacciones de pago que puede utilizar para la administración y la auditoría centralizadas. Esta documentación proporciona una descripción detallada de las operaciones criptográficas que puede utilizar en la criptografía de AWS pagos para ayudarle a evaluar las funciones que ofrece el servicio.

AWS La criptografía de pagos contiene varias interfaces (incluida una RESTful API, a través de la AWS CLI, el AWS SDK y el Consola de administración de AWS) para solicitar operaciones criptográficas de una flota distribuida de módulos de seguridad de hardware validados por PCI PTS HSM.



AWS La criptografía de pagos es un servicio escalonado que consta de hosts de criptografía de AWS pagos con acceso a la web y un nivel de. HSMs La agrupación de estos servidores en niveles forma la pila de criptografía de pagos. AWS Todas las solicitudes de criptografía de AWS pagos deben realizarse mediante el protocolo de seguridad de la capa de transporte (TLS) y finalizarse en un servidor de criptografía de pagos. AWS Los hosts del servicio solo permiten el uso de TLS con un conjunto de cifrado que proporciona una confidencialidad total. El servicio autentica y autoriza sus solicitudes mediante los mismos mecanismos de credenciales y políticas de IAM que están disponibles para todas las demás operaciones de la API. AWS

AWS Los servidores de criptografía de pagos se conectan al HSM subyacente a través de una red privada no virtual. Las conexiones entre los componentes del servicio y el HSM están protegidas con TLS mutuos (mTLS) para la autenticación y el cifrado.

Temas

- Objetivos de diseño
- Principios básicos
- Operaciones internas
- Operaciones de clientes

Objetivos de diseño

AWS La criptografía de pagos está diseñada para cumplir los siguientes requisitos:

- Confiable: el uso de las claves está protegido por las políticas de control de acceso que usted define y administra. No existe ningún mecanismo para exportar claves de criptografía de AWS pagos en texto plano. La confidencialidad de las claves criptográficas es crucial. Se requieren varios empleados de Amazon con acceso específico a los controles de acceso basados en quórums para realizar acciones administrativas en el. HSMs Ningún empleado de Amazon tiene acceso a las claves principales (o maestras) ni a las copias de seguridad de HSM. No se pueden sincronizar las claves principales HSMs que no formen parte de una región de criptografía de pagos. AWS Todas las demás claves están protegidas por las claves principales de HSM. Por lo tanto, las claves AWS de criptografía de pago de los clientes no se pueden utilizar fuera del servicio de criptografía de AWS pagos que opera en la cuenta del cliente.
- Baja latencia y alto rendimiento: la criptografía de AWS pagos proporciona operaciones criptográficas a un nivel de latencia y rendimiento adecuado para gestionar las claves criptográficas de pago y procesar las transacciones de pago.
- Durabilidad: la durabilidad de las claves criptográficas está diseñada para igualar a la de los servicios de mayor durabilidad en AWS. Una única clave criptográfica puede compartirse con un terminal de pago, una tarjeta con chip EMV u otro dispositivo criptográfico seguro (DSC) que se utilice durante muchos años.
- Regiones independientes: AWS proporciona regiones independientes para los clientes que necesiten restringir el acceso a los datos en diferentes regiones o necesiten cumplir requisitos de residencia de datos. El uso de claves se puede aislar dentro de una región de AWS.
- Fuente segura de números aleatorios: dado que una criptografía sólida depende de una generación de números aleatorios realmente impredecible, la criptografía de AWS pagos proporciona una fuente de números aleatorios validada y de alta calidad. Toda la generación de claves para la criptografía AWS de pagos utiliza un HSM PCI PTS que cotiza en el HSM y funciona en modo PCI.

- Auditoría: la criptografía de AWS pagos registra el uso y la gestión de las claves criptográficas en CloudTrail los registros y registros de servicio disponibles en Amazon. CloudWatch Puedes usar CloudTrail los registros para inspeccionar el uso de tus claves criptográficas, incluido el uso de las claves por parte de las cuentas con las que has compartido claves. AWS La criptografía de pagos es auditada por asesores externos según las normas PCI aplicables, la marca de la tarjeta y la seguridad de los pagos regionales. Las Certificaciones y las guías de Responsabilidad compartida están disponibles en AWS Artifact.
- Elastic: la criptografía de AWS pagos se amplía y amplía según su demanda. En lugar de predecir y reservar la capacidad de HSM, Payment Cryptography ofrece criptografía AWS de pagos bajo demanda. AWS La criptografía de pagos asume la responsabilidad de mantener la seguridad y la conformidad del HSM a fin de proporcionar la capacidad suficiente para satisfacer los picos de demanda de los clientes.

Principios básicos

Los temas de este capítulo describen las primitivas criptográficas de la criptografía de AWS pagos y dónde se utilizan. También presentan los elementos básicos del servicio.

Temas

- Primitivas criptográficas
- Entropía y generación de números aleatorios
- Operaciones de clave simétrica
- Operaciones con claves asimétricas
- Almacenamiento de claves
- Importación de claves simétricas
- Importación de claves con claves asimétricas
- Exportación de claves
- Protocolo de clave única derivada por transacción (DUKPT)
- Jerarquía de claves

Primitivas criptográficas

AWS La criptografía de pagos utiliza algoritmos criptográficos estándar parametrizables para que las aplicaciones puedan implementar los algoritmos necesarios para su caso de uso. El conjunto

de algoritmos criptográficos está definido por las normas PCI, ANSI X9 e ISO. EMVco Toda la criptografía se realiza mediante el PCI PTS HSM, que cotiza en el estándar y se ejecuta en modo PCI. HSMs

Entropía y generación de números aleatorios

AWS La generación de claves de criptografía de pago se realiza en la criptografía de pago. AWS HSMs HSMs Implemente un generador de números aleatorios que cumpla con el requisito PCI PTS HSM para todos los tipos y parámetros de clave compatibles.

Operaciones de clave simétrica

Se admiten los algoritmos de clave simétrica y los valores de clave definidos en ANSI X9 TR 31, ANSI X9.24 y PCI PIN Anexo C:

- Funciones hash: algoritmos de la SHA3 familia SHA2 y con un tamaño de salida superior a 2551. Excepto para la retrocompatibilidad con terminales POI v3 anteriores al PTS PCI.
- Cifrado y descifrado: AES con tamaño de clave mayor o igual a 128 bits, o TDEA con tamaño de clave mayor o igual a 112 bits (2 claves o 3 claves).
- Códigos de autenticación de mensajes (MACs) CMAC o GMAC con AES, así como HMAC con una función de hash aprobada y un tamaño de clave superior o igual a 128.

AWS La criptografía de pagos utiliza el AES 256 para las claves principales del HSM, las claves de protección de datos y las claves de sesión TLS.

Nota: Algunas de las funciones enumeradas se utilizan internamente para admitir protocolos y estructuras de datos estándar. Consulte la documentación de la API para ver los algoritmos compatibles con acciones específicas.

Operaciones con claves asimétricas

Se admiten los algoritmos de clave asimétrica y los valores de clave definidos en ANSI X9 TR 31, ANSI X9.24 y PCI PIN Anexo C:

- Esquemas de establecimiento clave aprobados, tal como se describe en el NIST SP8 00-56A (). ECC/FCC2-based key agreement), NIST SP800-56B (IFC-based key agreement), and NIST SP800-38F (AES-based key encryption/wrapping

AWS Los servidores de criptografía de pagos solo permiten las conexiones al servicio mediante TLS con un conjunto de cifrado que proporciona un secreto total.

Nota: Algunas de las funciones enumeradas se utilizan internamente para admitir protocolos y estructuras de datos estándar. Consulte la documentación de la API para ver los algoritmos compatibles con acciones específicas.

Almacenamiento de claves

AWS Las claves de criptografía de pago están protegidas por las claves principales del HSM AES 256 y se almacenan en bloques de claves ANSI X9 TR 31 en una base de datos cifrada. La base de datos se replica en la base de datos en memoria de los servidores de criptografía de pagos. AWS

Según el Anexo C de la Normativa de seguridad PIN de la PCI, las claves AES 256 son igual o más fuertes que:

- TDEA de 3 claves
- RSA de 15360 bits
- ECC de 512 bits
- DSA, DH y MQV 15360/512

Importación de claves simétricas

AWS La criptografía de pagos permite la importación de criptogramas y bloques de claves con claves simétricas o públicas con una clave de cifrado de clave simétrica (KEK) igual o más segura que la clave protegida para la importación.

Importación de claves con claves asimétricas

AWS La criptografía de pagos permite la importación de criptogramas y bloques de claves con claves simétricas o públicas protegidas por una clave de cifrado de clave privada (KEK) igual o más segura que la clave protegida para la importación. La clave pública proporcionada para el descifrado debe tener su autenticidad e integridad garantizadas por un certificado de una autoridad de confianza del cliente.

Las KEK públicas que proporciona AWS Payment Cryptography cuentan con la protección de autenticación e integridad de una autoridad de certificación (CA) que certifica el cumplimiento de las normas PCI PIN Security y del anexo A de la PCI P2PE.

Exportación de claves

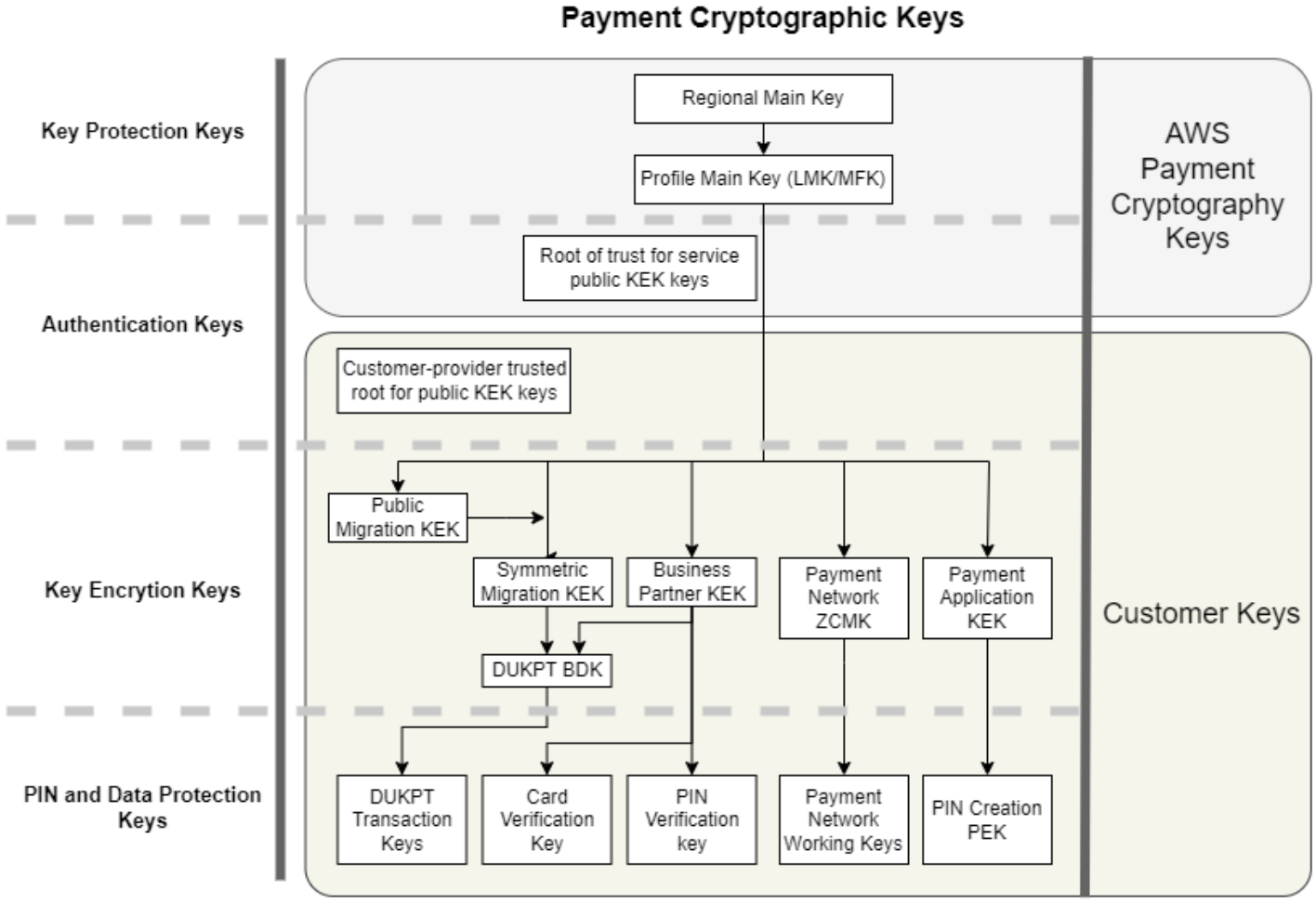
Las claves se pueden exportar y proteger con las claves adecuadas KeyUsage y que sean igual o más seguras que la clave que se va a exportar.

Protocolo de clave única derivada por transacción (DUKPT)

AWS La criptografía de pagos es compatible con las claves de derivación base (BDK) TDEA y AES, tal como se describe en la norma ANSI X9.24-3.

Jerarquía de claves

La jerarquía de claves de criptografía de AWS pagos garantiza que las claves estén siempre protegidas por claves tan sólidas o más sólidas que las claves que protegen.



AWS Las claves de criptografía de pago se utilizan para la protección de las claves dentro del servicio:

Key	Description (Descripción)
Clave principal regional	Protege las imágenes virtuales del HSM, o perfiles, utilizadas para el procesamiento criptográfico. Esta clave sólo existe en el HSM y en las copias de seguridad.
Clave principal de perfil	Clave de protección de claves de cliente de nivel superior, tradicionalmente denominada clave maestra local (LMK) o clave maestra de archivo (MFK) para las claves de cliente. Esta clave sólo existe en el HSM y en las copias de seguridad. Los perfiles definen distintas configuraciones del HSM según lo requieran las normas de seguridad para los casos de uso de pagos.
Raíz de confianza para las claves de cifrado de clave pública (KEK) de criptografía de AWS pagos	La clave pública raíz de confianza y el certifica do para autenticar y validar las claves públicas proporcionados por AWS Payment Cryptogra phy para la importación y exportación de claves mediante claves asimétricas.

Las claves de cliente se agrupan por claves utilizadas para proteger otras claves y claves que protegen datos relacionados con el pago. Estos son ejemplos de claves de cliente de ambos tipos:

Key	Description (Descripción)
Raíz de confianza proporcionada por el cliente para claves públicas KEK	Clave pública y certificado proporcionados por usted como raíz de confianza para autenticar y validar las claves públicas que usted suministr a para la importación y exportación de claves utilizando claves asimétricas.
Claves de cifrado de claves (KEK)	Las KEK se utilizan únicamente para cifrar otras claves para su intercambio entre almacenes de claves externos y AWS Payment

Key	Description (Descripción)
	Cryptography, socios comerciales, redes de pago o diferentes aplicaciones de su organizac ión.
Clave derivada única por transacción (DUKPT) clave derivada base (BDK)	BDKs se utilizan para crear claves únicas para cada terminal de pago y convertir las transacci ones de varios terminales en una única clave funcional del banco adquirente o del adquirent e. La mejor práctica, que exige el Point-to-Point cifrado PCI (P2PE), es utilizar diferentes tipos de terminales para distintos BDKs modelos de terminales, servicios de inyección o inicializ ación de claves u otros tipos de segmentac ión para limitar el impacto de comprometer un BDK.
Clave maestra de control de zona de red de pagos (ZCMK)	Las ZCMK, también denominadas claves de zona o claves maestras de zona, son proporcio nadas por las redes de pago para establecer claves de trabajo iniciales.
Claves de transacción DUKPT	Los terminales de pago configurados para DUKPT obtienen una clave única para el terminal y la transacción. El HSM que recibe la transacción puede determinar la clave a partir del identificador del terminal y del número de secuencia de la transacción.

Key	Description (Descripción)
Claves de preparación de datos de tarjetas	Las claves maestras del emisor EMV, las claves y valores de verificación de la tarjeta EMV y las claves de protección del archivo de datos de personalización de la tarjeta se utilizan para crear datos de tarjetas individua les para su uso por un proveedor de personali zación de tarjetas. Estas claves y los datos criptográficos de validación también son utilizados por los bancos emisores, o emisores, para autenticar los datos de las tarjetas como parte de la autorización de las transacciones.
Claves de preparación de datos de tarjetas	Las claves maestras del emisor EMV, las claves y valores de verificación de la tarjeta EMV y las claves de protección del archivo de datos de personalización de la tarjeta se utilizan para crear datos de tarjetas individua les para su uso por un proveedor de personali zación de tarjetas. Estas claves y los datos criptográficos de validación también son utilizados por los bancos emisores, o emisores, para autenticar los datos de las tarjetas como parte de la autorización de las transacciones.
Claves de trabajo de la red de pago	A menudo denominadas clave de trabajo del emisor o clave de trabajo del adquirente, son las claves que cifran las transacciones enviadas a las redes de pago o recibidas de ellas. Estas claves son rotadas con frecuencia por la red, a menudo diariamente o cada hora. Se trata de claves de cifrado con PIN (PEK) para las transacciones. PIN/Debit

Key	Description (Descripción)
Claves de cifrado (PEK) del número de identific ación personal (PIN)	Las aplicaciones que crean o descifran bloques de PIN utilizan PEK para evitar el almacenam iento o la transmisión del PIN en texto claro.

Operaciones internas

Este tema describe los requisitos internos implementados por el servicio para asegurar las claves de los clientes y las operaciones criptográficas para un servicio de criptografía de pagos y gestión de claves distribuido y escalable a nivel mundial.

Temas

- Protección HSM
- Administración general de claves
- Gestión de las claves de los clientes
- Seguridad de las comunicaciones
- Registro y supervisión

Protección HSM

Especificaciones y ciclo de vida del HSM{

AWS La criptografía de pagos utiliza una flota de productos disponibles en el mercado. HSMs HSMs Están validados por el FIPS 140-2 de nivel 3 y también utilizan versiones de firmware y la política de seguridad que figuran en la lista de dispositivos PCI PTS aprobada por el Consejo de Normas de Seguridad PCI como compatibles con PCI HSM v3. La norma PCI PTS HSM incluye requisitos adicionales para la fabricación, el envío, la implementación, la gestión y la destrucción del hardware HSM que son importantes para la seguridad y el cumplimiento de los pagos pero que no están contemplados en FIPS 140.

Los asesores externos comprueban la marca, el modelo, el firmware, la configuración, la gestión física del ciclo de vida, el control de cambios, los controles de acceso de los operadores, la gestión de las claves principales y todos los requisitos de PCI PIN y P2PE relacionados con las operaciones del HSM. HSMs

Todos funcionan en modo PCI y HSMs se configuran con la política de seguridad PCI PTS HSM. Solo están habilitadas las funciones necesarias para admitir los casos AWS de uso de la criptografía de pagos. AWS La criptografía de pagos no permite imprimir, mostrar ni devolver texto sin cifrar. PINs

Seguridad física del dispositivo HSM

El servicio solo podrá utilizar aquellos dispositivos HSMs que cuenten con las claves del dispositivo firmadas por una autoridad certificadora de criptografía de AWS pagos (CA) por el fabricante antes de la entrega. La criptografía de AWS pagos es una subentidad de certificación de la entidad emisora de certificados del fabricante y constituye la base de confianza de los certificados de fabricante y dispositivo de HSM. La CA del fabricante ha certificado el cumplimiento del anexo A de seguridad PCI PIN y el anexo A de PCI P2PE. El fabricante verifica que todos los HSM con claves de dispositivo firmadas por la CA de criptografía de AWS pagos se envíen al receptor designado de AWS.

Tal y como exige la seguridad PCI PIN, el fabricante suministra una lista de números de serie a través de un canal de comunicación distinto al del envío del HSM. Estos números de serie se comprueban en cada paso del proceso de instalación del HSM en los centros de datos de AWS. Por último, los operadores AWS de criptografía de pago validan la lista de HSM instalados comparándola con la lista del fabricante antes de añadir el número de serie a la lista de HSM autorizados a recibir claves de criptografía de pago. AWS

HSMs están guardadas de forma segura o bajo un doble control en todo momento, lo que incluye:

- El envío desde el fabricante a una instalación de montaje en bastidor de AWS.
- Durante el montaje en bastidor.
- Envío desde la instalación de montaje en bastidor a un centro de datos.
- Recepción e instalación en una sala de procesamiento segura de un centro de datos. Los bastidores HSM aplican un doble control con cerraduras de acceso controlado por tarjeta, sensores de puerta con alarma y cámaras.
- Durante las operaciones.
- Durante el desmantelamiento y la destrucción.

Se mantiene y supervisa un sistema completo chain-of-custody, con responsabilidad individual, para cada HSM.

Inicialización de HSM

Un HSM solo se inicializa como parte del conjunto de criptografía de AWS pagos después de validar su identidad e integridad mediante los números de serie, las claves de dispositivo instaladas por el fabricante y la suma de verificación del firmware. Una vez validada la autenticidad e integridad de un HSM, se configura, incluyendo la habilitación del Modo PCI. A continuación, se establecen las claves principales de la región de criptografía de AWS pagos y las claves principales del perfil, y el HSM queda a disposición del servicio.

Servicio y reparación del HSM

Los HSM tienen componentes reparables que no requieren la violación del límite criptográfico del dispositivo. Estos componentes incluyen ventiladores de refrigeración, fuentes de alimentación y baterías. Si un HSM u otro dispositivo dentro del bastidor de HSM necesita servicio, se mantiene el control dual durante todo el periodo en que el bastidor está abierto.

Desactivación de HSM

El desmantelamiento se produce debido a un HSM end-of-life o a un fallo de éste. Los HSM se ponen a cero de forma lógica antes de sacarlos de su rack, si están en funcionamiento, y luego se destruyen en las salas de procesamiento seguras de los centros de datos de AWS. Nunca se devuelven al fabricante para su reparación, ni se utilizan para otro fin, ni se sacan de otro modo de una sala de procesamiento segura antes de su destrucción.

Actualización del firmware del HSM

Las actualizaciones del firmware de HSM se aplican cuando es necesario mantener la alineación con las versiones incluidas en la lista PCI PTS HSM y FIPS 140-2 (o FIPS 140-3), si se trata de una actualización relacionada con la seguridad o si se determina que los clientes pueden beneficiarse de las funciones de una nueva versión. AWS Payment Cryptography HSMs ejecuta off-the-shelf el firmware que coincide con las versiones PCI PTS incluidas en la lista HSM. La integridad de las nuevas versiones de firmware se valida con las versiones de firmware certificadas por PCI o FIPS y, a continuación, se comprueba su funcionalidad antes de lanzarlas a todas. HSMs

Acceso del operador

Los operadores pueden tener acceso no consular a los HSM para la resolución de problemas en los raros casos en que la información recopilada de los HSM durante las operaciones normales sea insuficiente para identificar un problema o planificar un cambio. Se ejecutan los siguientes pasos:

- Se desarrollan y aprueban las actividades de resolución de problemas y se programa la sesión no consular.
- Se retira un HSM del servicio de procesamiento del cliente.
- Se eliminan las claves principales, bajo doble control.
- Se permite al operador el acceso no consular al HSM para realizar las actividades de resolución de problemas aprobadas, bajo control dual.
  - Tras la finalización de la sesión no consular, se realiza el proceso de aprovisionamiento inicial en el HSM, devolviendo el firmware y la configuración estándar y sincronizando la clave principal, antes de devolver el HSM al servicio de los clientes.
  - Los registros de la sesión se graban en el seguimiento de cambios.
  - La información obtenida de la sesión se utiliza para planificar futuros cambios.

Todos los registros de acceso ajenos a la consola se revisan para comprobar la conformidad con los procesos y los posibles cambios en la supervisión del HSM, el proceso de non-console-access gestión o la formación de los operadores.

Administración general de claves

Todos los HSM de una región se sincronizan con una clave principal de región. Una clave principal de región protege al menos una clave principal de perfil. Una clave principal de perfil protege claves de cliente.

Todas las claves principales son generadas por un HSM y distribuidas a mediante la distribución de claves simétricas utilizando técnicas asimétricas, alineadas con ANSI X9 TR 34 y PCI PIN Anexo A.

Generación

Las claves principales AES de 256 bits se generan en uno de los HSM aprovisionados para la flota de HSM de servicio, utilizando el generador de números al azar PCI PTS HSM.

Sincronización de la clave principal de región

Las claves principales de la región HSM son sincronizadas por el servicio en toda la flota regional con mecanismos definidos por ANSI X9 TR-34, que incluyen:

- Autenticación mutua mediante claves del host de distribución de claves (KDH) y del dispositivo receptor de claves (KRD) y certificados para proporcionar autenticación e integridad de las claves públicas.

- Los certificados están firmados por una autoridad de certificación (CA) que cumple los requisitos del Anexo A2 del PIN de la PCI, excepto para los algoritmos asimétricos y las intensidades de clave apropiadas para proteger las claves AES de 256 bits.
- La identificación y la protección de las claves simétricas distribuidas son compatibles con la norma ANSI X9 TR-34 y el PCI PIN anexo A1, excepto en lo que respecta a los algoritmos asimétricos y las intensidades de las teclas adecuadas para proteger las claves AES de 256 bits.

Las claves principales de la región se establecen para las HSMs que se han autenticado y aprovisionado para una región mediante:

- Se genera una clave principal en un HSM de la región. Ese HSM se designa como host de distribución de claves.
- Todas las provisiones HSMs en la región generan un token de autenticación KRD, que contiene la clave pública del HSM e información de autenticación que no se puede reproducir.
- Los tokens KRD se añaden a la lista de permitidos del KDH después de que éste valide la identidad y el permiso del HSM para recibir claves.
- El KDH produce un token de clave principal autenticable para cada HSM. Los tokens contienen la información de autenticación del KDH y la clave principal cifrada que sólo se puede cargar en el HSM para el que se ha creado.
- A cada HSM se le envía el token de clave principal creado para él. Tras validar la información de autenticación propia del HSM y la información de autenticación del KDH, la clave principal se descifra mediante la clave privada del KRD y se carga en la clave principal.

En caso de que un único HSM deba volver a sincronizarse con una región:

- Se vuelve a validar y se aprovisiona con firmware y configuración.
- Si es nuevo en la región:
  - El HSM genera un token de autenticación KRD.
  - El KDH añade el token a su lista de permitidos.
  - El KDH genera un token de clave principal para el HSM.
  - El HSM carga la clave principal.
  - El HSM se pone a disposición del servicio.

Esto garantiza que:

- Solo los HSM validados para el procesamiento de criptografía AWS de pagos en una región pueden recibir la clave maestra de esa región.
- Solo se puede distribuir una clave maestra de un HSM de criptografía de AWS pagos a un HSM de la flota.

Rotación de la clave principal de la región

Las claves principales de región se rotan al expirar el periodo de criptografía, en el improbable caso de que se sospeche que la clave está comprometida, o tras cambios en el servicio que se determine que afectan a la seguridad de la clave.

Se genera y distribuye una nueva clave principal de región como en la provisión inicial. Las claves principales de perfil guardadas deben traducirse a la nueva clave principal de región.

La rotación de la clave principal de región no afecta al procesamiento del cliente.

Sincronización de la clave principal de perfil

Las claves principales de perfil están protegidas por las claves principales de región. Esto restringe un perfil a una región específica.

Las claves principales de perfil se aprovisionan en consecuencia:

- Se genera una clave principal de perfil en un HSM que tenga sincronizada la clave principal de región.
- La clave principal del perfil se almacena y encripta con la configuración del perfil y otros contextos.
- El perfil es utilizado para las funciones criptográficas del cliente por cualquier HSM de la región con la clave principal de la región.

Rotación de la clave principal del perfil

Las claves principales de perfil se rotan al expirar el periodo criptográfico, tras sospecha de compromiso de la clave o tras cambios en el servicio que se determine que afectan a la seguridad de la clave.

Pasos de la rotación:

- Se genera una nueva clave principal de perfil y se distribuye como clave principal pendiente al igual que con la provisión inicial.

- Un proceso en segundo plano traduce el material de la clave de cliente de la clave principal de perfil establecida a la clave principal pendiente.
- Cuando todas las claves de cliente se han cifrado con la clave pendiente, ésta se promueve a clave principal de perfil.
- Un proceso en segundo plano borra el material de las claves de cliente protegido por la clave pendiente.

La rotación de la clave principal del perfil no afecta al procesamiento de los clientes.

Protección

Las claves sólo dependen de la jerarquía de claves para su protección. La protección de las claves principales es fundamental para evitar la pérdida o el compromiso de todas las claves de cliente.

Las claves principales de región son restaurables desde la copia de seguridad sólo para HSM autenticados y aprovisionados para el servicio. Estas claves sólo pueden almacenarse como tokens de clave principal mutuamente autenticables y cifrados de un KDH específico para un HSM específico.

Las claves principales de perfil se almacenan con la configuración del perfil y la información de contexto encriptada por región.

Las claves de cliente se almacenan en bloques de claves, protegidos por una clave maestra de perfil.

Todas las claves existen exclusivamente dentro de un HSM o se almacenan protegidas por otra clave de igual o mayor fuerza criptográfica.

Durabilidad

Las claves de cliente para la criptografía de las transacciones y las funciones empresariales deben estar disponibles incluso en situaciones extremas que suelen provocar interrupciones. AWS La criptografía de pagos utiliza un modelo de redundancia de varios niveles en todas las zonas y regiones de disponibilidad. AWS Los clientes que requieran una mayor disponibilidad y durabilidad para las operaciones criptográficas de pago que la proporcionada por el servicio deberán implementar arquitecturas multirregión.

Los tokens de autenticación del HSM y de la clave principal se guardan y pueden utilizarse para restaurar una clave principal o sincronizarse con una nueva clave principal, en caso de que deba

restablecerse un HSM. Los tokens se archivan y sólo se utilizan bajo doble control cuando es necesario.

El operador accede a las claves principales de HSM

Las claves principales solo existen en el HSM administrado por el servicio y protegido en instalaciones seguras de AWS. Las claves principales no se pueden exportar desde ningún HSM ni sincronizarse con un HSM que no esté inicializado por el fabricante para su uso en el servicio. Los operadores de AWS no pueden obtener claves principales de ninguna forma que puedan cargarse en un HSM no administrado por el servicio.

Gestión de las claves de los clientes

En AWS, la confianza del cliente es nuestra principal prioridad. Usted mantiene el control total de las claves que importe o cree en el servicio en su cuenta de AWS. Usted es responsable de configurar el acceso a las claves.

AWS Payment Cryptography es un proveedor de servicios que usa HSMs y administra las claves en nombre de los clientes, de forma similar a los proveedores de servicios de pago tradicionales. El servicio es totalmente responsable de la seguridad física y lógica de HSM. La responsabilidad de administrar las claves la comparten el servicio y los clientes, ya que el cliente debe proporcionar información precisa sobre las claves creadas por el servicio o importadas al mismo, que el servicio utiliza para garantizar el uso y la administración correctos de las claves. Las protecciones de segregación de datos de AWS se utilizan para garantizar que las claves que pertenecen a una cuenta de AWS no puedan comprometer las claves que pertenecen a otra.

AWS Payment Cryptography es plenamente responsable de la conformidad física del HSM y de la administración de claves de las claves gestionadas por el servicio. Esto requiere la propiedad y la administración de las claves principales del HSM y la protección de las claves de los clientes gestionadas mediante la AWS criptografía de pagos.

Separación del espacio de claves del cliente

AWS La criptografía de pagos aplica políticas clave para todos los usos de las claves, incluida la limitación del capital a la cuenta propietaria de la clave, a menos que una clave se comparta explícitamente con otra cuenta.

Las cuentas de AWS proporcionan una segregación completa del entorno entre clientes o aplicaciones de forma análoga a las implementaciones no basadas en la nube en diferentes centros de datos. Cada cuenta proporciona control de acceso aislado, redes, recursos informáticos,

almacenamiento de datos, claves criptográficas para la protección de datos y las transacciones de pago, y todos los recursos de AWS. Los servicios de AWS, como Organizations y Control Tower, permiten la administración empresarial de cuentas de aplicaciones independientes, de forma análoga a las jaulas o salas de un centro de datos empresarial.

El operador accede a las claves de los clientes

Las claves de cliente gestionadas por el servicio se almacenan protegidas por las claves principales de la partición y solo las puede utilizar la cuenta del cliente propietario o la cuenta que el propietario haya configurado específicamente para compartir las claves. Los operadores de AWS no pueden exportar ni realizar operaciones criptográficas o de administración de claves con las claves de los clientes mediante el acceso manual al servicio, que se administra mediante los mecanismos de acceso manual de los operadores de AWS.

El código de servicio que implementa la administración y el uso de las claves del cliente está sujeto a las prácticas de código seguro de AWS, según se evalúa en la evaluación PCI DSS de AWS.

Copia de seguridad y recuperación

Las claves y la información clave almacenadas internamente por el servicio para una región se guardan en archivos cifrados mediante. AWS Los archivos requieren un doble control AWS para restaurarlos.

Bloques de claves

Todas las claves se almacenan y procesan en bloques de claves con formato ANSI X9.143.

Las claves se pueden importar al servicio desde criptogramas u otros formatos de bloques de claves compatibles con. ImportKey Del mismo modo, las claves pueden exportarse, si son exportables, a otros formatos de bloques de claves o criptogramas soportados por perfiles de exportación de claves.

Uso de claves

El uso de claves está restringido a lo configurado KeyUsage por el servicio. El servicio fallará cualquier solicitud con un uso de clave, modo de uso o algoritmo inapropiados para la operación criptográfica solicitada.

Relaciones de intercambio de claves

PCI PIN Security y PCI P2PE exigen que las organizaciones que comparten claves que cifran PINs o archivan datos, incluidas las claves de intercambio de claves (KEK) utilizadas para compartir esas

claves, no compartan las mismas claves con ninguna otra organización. Se recomienda que las claves simétricas se compartan solo entre dos partes con un único propósito, incluso dentro de la misma organización. Esto minimiza el impacto de presuntos compromisos de claves que obliguen a reemplazar las claves afectadas.

Incluso los casos empresariales que requieren compartir claves entre más de 2 partes, deben mantener el número de partes al mínimo.

AWS La criptografía de pagos proporciona etiquetas clave que se pueden usar para rastrear y hacer cumplir el uso de las claves dentro de esos requisitos.

Por ejemplo, las claves KEK y BDK para diferentes instalaciones de inyección de claves se pueden identificar configurando «KIF» = «POSStation» para todas las claves compartidas con ese proveedor de servicios. Otro ejemplo sería etiquetar las claves compartidas con las redes de pago con «Network» = «PayCard». El etiquetado le permite crear controles de acceso y crear informes de auditoría para hacer cumplir y demostrar sus prácticas de gestión de claves.

Eliminación de claves

DeleteKey marca las claves de la base de datos para eliminarlas después de un período configurable por el cliente. Transcurrido este periodo, la llave se borra irremediablemente. Se trata de un mecanismo de seguridad para evitar el borrado accidental o malintencionado de una clave. Las claves marcadas para su eliminación no están disponibles para ninguna acción excepto: RestoreKey

Las llaves borradas permanecen en las copias de seguridad del servicio durante 7 días después de su borrado. No son restaurables durante este periodo.

Las claves pertenecientes a cuentas AWS cerradas se marcan para su borrado. Si la cuenta se reactiva antes de que se alcance el periodo de borrado, las claves marcadas para borrado se restauran, pero se desactivan. Deberá volver a habilitarlas para poder utilizarlas en operaciones criptográficas.

Seguridad de las comunicaciones

Externo

AWS Los terminales de la API de criptografía de pagos cumplen con los estándares de AWS seguridad, como el TLS 1.2 o superior y la versión 4 de Signature para la autenticación e integridad de las solicitudes.

Las conexiones TLS entrantes se terminan en equilibradores de carga de red y se reenvían a los gestores de API a través de conexiones TLS internas.

Interno

Las comunicaciones internas entre componentes de servicio y entre componentes de servicio y otro servicio de AWS están protegidas por TLS utilizando criptografía fuerte.

Los HSM se encuentran en una red privada no virtual a la que sólo se puede acceder desde los componentes de servicio. Todas las conexiones entre los HSM y los componentes de servicio están protegidas con TLS mutuo (mTLS), igual o superior a TLS 1.2. Los certificados internos para TLS y mTLS son administrados por el Gestor de certificación de Amazon mediante una Autoridad de certificación privada de AWS. La red interna VPCs y la red HSM se supervisan para detectar actividades inesperadas y cambios de configuración.

Registro y supervisión

Los registros de servicios internos incluyen:

- CloudTrail registros de las llamadas al servicio de AWS realizadas por el servicio
- CloudWatch registros de ambos eventos registrados directamente en los CloudWatch registros o eventos de HSM
- Archivos de registro de HSM y sistemas de servicio
- Archivos de registro

Todas las fuentes de registros controlan y filtran la información confidencial, incluida la relativa a las claves. Los registros se revisan sistemáticamente para garantizar que no contienen información sensible de los clientes.

El acceso a los registros está restringido a las personas necesarias para completar las funciones de su trabajo.

Todos los registros se retienen de acuerdo con las políticas de conservación de registros de AWS.

Operaciones de clientes

AWS La criptografía de pagos es totalmente responsable del cumplimiento físico del HSM según las normas PCI. El servicio también proporciona un almacén de claves seguro y garantiza que las claves solo se puedan utilizar para los fines permitidos por los estándares PCI y que usted especifique

durante la creación o la importación. Usted es responsable de configurar los atributos clave y el acceso para aprovechar las capacidades de seguridad y cumplimiento del servicio.

Temas

- Generación de claves
- Importación de claves
- Exportación de claves
- Eliminación de claves de
- Rotar claves de

Generación de claves

Al crear las claves, debe establecer los atributos que el servicio utiliza para hacer cumplir el uso de la clave:

- Longitud de algoritmo y clave
- De uso
- Disponibilidad y vencimiento

Las etiquetas que se utilizan para el control de acceso basado en atributos (ABAC) se utilizan para limitar las claves para su uso con socios o aplicaciones específicos. Asegúrese de incluir políticas para limitar los roles permitidos para borrar o cambiar etiquetas.

Debe asegurarse de que las políticas que determinan los roles que pueden utilizar y gestionar la clave se establecen antes de la creación de la clave.

> **Note**
>
> Las políticas de IAM relativas a los CreateKey comandos se pueden utilizar para imponer y demostrar un doble control en la generación de claves.

Importación de claves

Al importar claves, el servicio establece los atributos para imponer el uso conforme de la clave utilizando la información criptográficamente vinculada del bloque de claves. El mecanismo para

establecer el contexto de clave fundamental consiste en utilizar bloques de claves creados con el HSM de origen y protegidos por un KEK compartido o asimétrico. Esto se ajusta a los requisitos del PCI PIN y preserva el uso, el algoritmo y la solidez de las claves de la aplicación de origen.

En el momento de la importación, se deben establecer los atributos clave, las etiquetas y las políticas de control de acceso importantes, además de la información del bloque clave.

La importación de claves mediante criptogramas no transfiere los atributos clave de la aplicación de origen. Debe configurar los atributos de forma adecuada utilizando este mecanismo.

A menudo, las claves se intercambian utilizando componentes de texto claro, se transmiten por los custodios de las claves y, a continuación, se cargan con la ceremonia que implementa el doble control en una sala segura. Esto no es compatible directamente con la criptografía de AWS pagos. La API exportará una clave pública con un certificado que puede ser importado por su propio HSM para exportar un bloque de claves que sea importable por el servicio. Esto permite utilizar su propio HSM para cargar componentes de texto no cifrado.

Debe utilizar los valores de comprobación de claves (KCV) para verificar que las claves importadas coinciden con las claves de origen.

Las políticas de IAM de la ImportKey API se pueden utilizar para aplicar y demostrar un doble control en la importación de claves.

Exportación de claves

Para compartir claves con socios o aplicaciones en las instalaciones, es posible que sea necesario exportar las claves. El uso de bloques clave para las exportaciones mantiene el contexto fundamental de las claves con el material de las claves cifradas.

Las etiquetas de las claves pueden utilizarse para limitar la exportación de claves a KEK que compartan la misma etiqueta y el mismo valor.

AWS La criptografía de pagos no proporciona ni muestra un texto claro sobre los componentes clave. Esto requiere el acceso directo de los custodios de claves a los dispositivos criptográficos seguros (SCD) probados por la PCI PTS HSM o la ISO 13491 para su visualización o impresión. Puede establecer una KEK asimétrica o una KEK simétrica con su SCD para llevar a cabo la ceremonia de creación de componentes clave de texto claro bajo doble control.

Los valores de comprobación clave (KCV) se deben utilizar para comprobar que los valores importados por el HSM de destino coinciden con las claves de origen.

Eliminación de claves de

Puede usar la API de eliminación de claves para programar la eliminación de las claves tras el período de tiempo que usted configure. Antes de ese momento, las claves se pueden recuperar. Una vez que se eliminan las claves, se eliminan permanentemente del servicio.

Las políticas de IAM de la DeleteKey API se pueden utilizar para aplicar y demostrar un doble control a la hora de eliminar las claves.

Rotar claves de

El efecto de la rotación de claves puede implementarse utilizando alias de claves creando o importando una nueva clave y modificando después el alias de claves para que haga referencia a la clave nueva. La clave anterior se eliminaría o deshabilitaría, según sus prácticas de administración.

Cuotas para AWS Payment Cryptography

La cuenta de AWS tiene cuotas predeterminadas para cada servicios de AWS (estas cuotas se denominaban anteriormente “límites”). A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Name	Valor predeterminado	Ajusta	Description (Descripción)
Alias	Cada región admitida: 2000	Sí	El número máximo de alias que puede tener en esta cuenta en la región actual.
Tasa combinada de solicitudes de plano de control	Cada región admitida: 5 por segundo	Sí	El número máximo de solicitudes de plano de control por segundo que puede realizar en esta cuenta en la región actual. Esta cuota se aplica a todas las operaciones del plano de control combinadas.
Tasa combinada de solicitudes de planos de datos (asimétrica)	Cada región admitida: 20 por segundo	Sí	El número máximo de solicitudes por segundo para operaciones en el plano de datos con una clave asimétric a que puede realizar en esta cuenta en la región actual. Esta cuota se aplica a todas las operaciones del plano de datos combinadas.

Name	Valor predeterminado	Ajusta	Description (Descripción)
Tasa combinada de solicitudes de planos de datos (simétrica)	Cada región admitida: 500 por segundo	Sí	El número máximo de solicitudes por segundo para operaciones de plano de datos con una clave simétrica que puede realizar en esta cuenta en la región actual. Esta cuota se aplica a todas las operaciones del plano de datos combinadas.
Claves	Cada región admitida: 2000	Sí	El número máximo de claves que puede tener en esta cuenta en la región actual, excluyendo las claves eliminadas.

Historial de documentos de la Guía del usuario AWS de criptografía de pagos

En la siguiente tabla se describen las versiones de la documentación sobre criptografía de AWS pagos.

Cambio	Descripción	Fecha
Nueva función - AS2805	Soporte para algoritmos y flujos para respaldar el apoyo AS2805 regional	17 de diciembre de 2025
Nueva función: replicación de claves multirregional	Con la replicación de claves multirregional, puede replicar sus claves de criptografía AWS de pagos en varias. Regiones de AWS	10 de septiembre de 2025
Nueva función: ECDH	Con esta versión, el ECDH se puede utilizar para establecer una KEK compartida para un mayor intercambio de claves.	30 de marzo de 2025
Nueva guía de intercambio de claves	Se proporciona una nueva guía para los intercamb ios clave. También se agregó información sobre los comandos comunes de JCB.	31 de enero de 2025
Lanzamiento de una nueva región	Se agregaron puntos finales para el lanzamiento de una nueva región en Europa (Fráncfort), Europa (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio)	31 de julio de 2024

CloudTrail para Data Plane y Dynamic Keys	Se agregó información sobre CloudTrail su utilización en operaciones de plano de datos (criptográficas), incluidos ejemplos. También se agregó información sobre el uso de claves dinámicas para determinadas funciones, a fin de admitir mejor las claves de un solo uso o de uso limitado que no deben importarse a la criptografía de AWS pagos	10 de julio de 2024
Ejemplos actualizados	Se agregaron nuevos ejemplos para la emisión de tarjetas	1 de julio de 2024
Lanzamiento de funciones	Añadir información sobre los puntos finales de la VPC (PrivateLink) y ejemplos de iCVV.	30 de mayo de 2024
Lanzamiento de funciones	Se agregó información sobre las nuevas funciones relacionadas con el import/export uso de claves RSA y la exportación de claves DUKPT IPEK/IK .	15 de enero de 2024
Versión inicial	Versión inicial de la Guía del usuario sobre criptografía de AWS pagos	8 de junio de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.