Leitfaden für Partner und Kunden

Secure Packager and Encoder Key Exchange API-Spezifikation

Secure Packager and Encoder Key Exchange API-Spezifikation: Leitfaden für Partner und Kunden

Table of Contents

Was ist Secure Packager und Encoder Key Exchange? 1
Allgemeine Architektur 1
Cloud-basierte AWS-Architektur 2
Erste Schritte 3
Bist du neu bei SPEKE? 4
Verwandte Serviceinformationen und Spezifikationen 4
Terminologie 4
Kunden-Onboarding 6
Beginnen Sie mit einem DRM-Plattformanbieter 6
SPEKE-Support für AWS-Services und -Produkte 7
SPEKE-Support für Services und Produkte von AWS-Partnern 8
SPEKE API-Spezifikation 9
Für SPEKE ist eine Authentifizierung erforderlich 10
Authentifizierung für AWS-Cloud-Implementierungen 10
Authentifizierung für lokale Produkte 11
SPEKE API v1 12
SPEKE API v1 — Anpassungen und Einschränkungen der DASH-IF-Spezifikation 13
SPEKE API v1 — Standard-Payload-Komponenten 14
SPEKE API v1 — Beispiele für Live-Workflow-Methodenaufrufe 17
SPEKE API v1 — Beispiele für VOD-Workflow-Methodenaufrufe 22
SPEKE API v1 — Inhaltsschlüsselverschlüsselung 26
SPEKE API v1 — Heartbeat 29
SPEKE API v1 — Überschreiben der Schlüssel-ID 30
SPEKE API v2 31
SPEKE API v2 — Anpassungen und Einschränkungen der DASH-IF-Spezifikation 33
SPEKE API v2 — Standard-Payload-Komponenten 37
SPEKE API v2 - Verschlüsselungsvertrag 43
SPEKE API v2 — Beispiele für Live-Workflow-Methodenaufrufe 53
SPEKE API v2 — Beispiele für VOD-Workflow-Methodenaufrufe 59
SPEKE API v2 — Verschlüsselung von Inhaltsschlüsseln 64
SPEKE API v2 — Überschreiben der Schlüssel-ID 68
Lizenz für die SPEKE API-Spezifikation 70
Creative Commons Namensnennung — ShareAlike 4.0 Internationale öffentliche Lizenz 70
Dokumentverlauf 78

..... lxxxii

Was ist Secure Packager und Encoder Key Exchange?

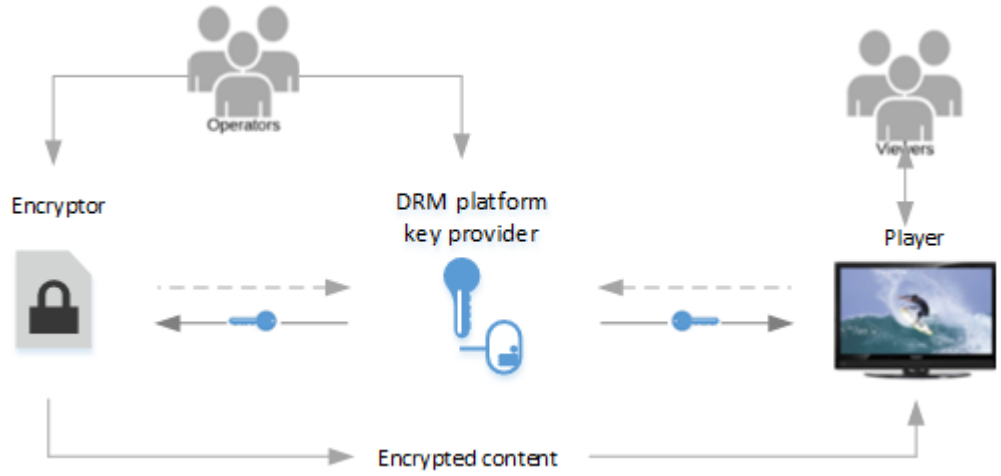
Secure Packager and Encoder Key Exchange (SPEKE) definiert den Standard für die Kommunikation zwischen Verschlüsselern und Paketierern von Medieninhalten und Anbietern von DRM-Schlüsseln (Digital Rights Management). Die Spezifikation berücksichtigt Verschlüsseler, die vor Ort und in der AWS-Cloud ausgeführt werden.

Themen

- Allgemeine Architektur
- Cloud-basierte AWS-Architektur
- Erste Schritte

Allgemeine Architektur

Die folgende Abbildung zeigt einen allgemeinen Überblick über die Architektur der SPEKE-Inhaltsverschlüsselung für lokale Produkte.



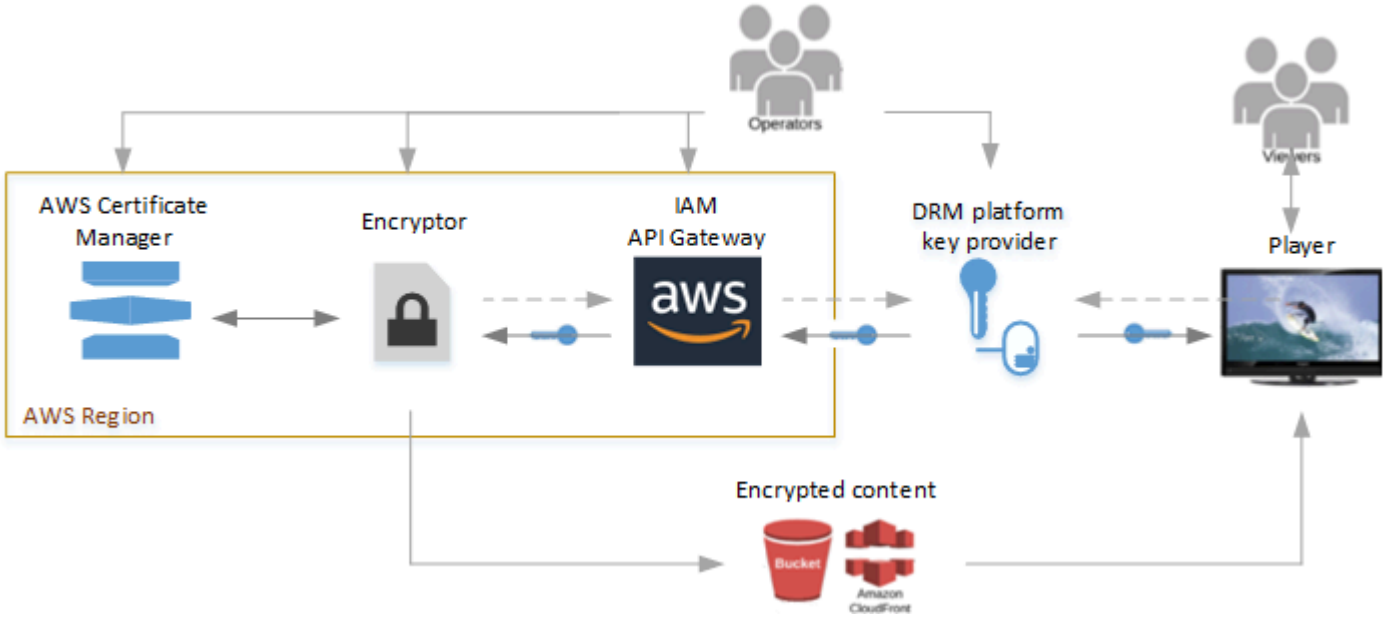
Dies sind die Hauptkomponenten der eben beschriebenen Architektur:

- Encryptor — Stellt die Verschlüsselungstechnologie bereit. Empfängt Verschlüsselungsanforderungen vom Operator und ruft die benötigten Schlüssel vom DRM-Schlüsselanbieter ab, um die verschlüsselten Inhalte zu sichern.
- Schlüsselanbieter für die DRM-Plattform — Stellt dem Verschlüsseler Verschlüsselungsschlüssel über eine SPEKE-konforme API zur Verfügung. Der Anbieter stellt außerdem Media-Playern Lizenzen für die Entschlüsselung bereit.

- Player — Fordert Schlüssel von demselben Schlüsselanbieter für die DRM-Plattform an, mit denen der Spieler die Inhalte freischaltet und sie seinen Zuschauern zur Verfügung stellt.

Cloud-basierte AWS-Architektur

Die folgende Abbildung zeigt die allgemeine Architektur, wenn SPEKE mit Services und Funktionen verwendet wird, die in der AWS Cloud ausgeführt werden.



Dies sind die Hauptservices und -komponenten:

- Encryptor — Stellt die Verschlüsselungstechnologie in der AWS-Cloud bereit. Der Verschlüsseler erhält Anfragen von seinem Operator und ruft die erforderlichen Verschlüsselungsschlüssel vom DRM-Schlüsselanbieter über Amazon API Gateway ab, um den verschlüsselten Inhalt zu sichern. Es liefert den verschlüsselten Inhalt an einen Amazon S3 S3-Bucket oder über eine CloudFront Amazon-Distribution.
- AWS IAM und Amazon API Gateway — Verwaltet Rollen, denen Kunden vertrauen, und die Proxykommunikation zwischen dem Verschlüsseler und dem Schlüsselanbieter. API Gateway stellt Protokollierungsfunktionen bereit und ermöglicht es Kunden, ihre Beziehungen mit dem Verschlüsseler und dem DRM-System zu steuern. Kunden ermöglichen den Zugriff auf den Schlüsselanbieter über die Konfiguration der IAM-Rolle. Das API Gateway muss sich in derselben AWS-Region wie der Verschlüsseler befinden.
- AWS Certificate Manager — (optional) Bietet Zertifikatsverwaltung für die Verschlüsselung von Inhaltsschlüsseln. Die Verschlüsselung von Inhaltsschlüsseln ist das empfohlene Verfahren, um die

Kommunikation zu sichern. Der Zertifikat-Manager muss sich in der gleichen AWS-Region wie der Verschlüsseler befinden.

- Schlüsselanbieter für die DRM-Plattform — Stellt dem Verschlüsseler Verschlüsselungsschlüssel über eine SPEKE-konforme API zur Verfügung. Der Anbieter stellt außerdem Media-Playern Lizenzen für die Entschlüsselung bereit.
- Player — Fordert Schlüssel von demselben Schlüsselanbieter für die DRM-Plattform an, mit denen der Spieler die Inhalte freischaltet und sie seinen Zuschauern zur Verfügung stellt.

Erste Schritte

Weiteres Einführungsmaterial zu SPEKE finden Sie unter Sind Sie neu bei SPEKE? .

Sind Sie Kunde?

Nehmen Sie Kontakt mit einem AWS Elemental-DRM-Plattformanbieter auf, damit die Verwendung der Verschlüsselung eingerichtet werden kann. Einzelheiten finden Sie unter Kunden-Onboarding.

Sind Sie ein DRM-Plattformanbieter oder ein Kunde mit Ihrem eigenen Schlüsselanbieter?

Stellen Sie eine REST-API für Ihren Schlüsselanbieter bereit, die der SPEKE-Spezifikation entspricht. Einzelheiten finden Sie in der SPEKE-API-Spezifikation.

Bist du neu bei SPEKE?

Dieser Abschnitt enthält einführende Informationen für Leser, die Secure Packager und Encoder Key Exchange (SPEKE) noch nicht kennen.

Eine Einführung in SPEKE finden Sie im folgenden Webcast:

Verwandte Serviceinformationen und Spezifikationen

- API-Gateway-Berechtigungen — So kontrollieren Sie den Zugriff auf eine API mit AWS Identity and Access Management (AWS IAM) -Berechtigungen.
- AWS AssumeRole — So verwenden Sie den AWS Security Token Service (AWS STS), um Rollenfunktionen zu übernehmen.
- AWS Sigv4 — So signieren Sie eine HTTP-Anfrage mit Signature Version 4.
- DASH-IF CPIX-Spezifikation v2.0 — Die Version der DASH-IF Content Protection Information Exchange Format (CPIX) -Spezifikation, auf der diese SPEKE v1.0-Spezifikation basiert.
- DASH-IF CPIX-Spezifikation v2.3 — Die DASH-IF Content Protection Information Exchange Format (CPIX) -Spezifikationsversion, auf der diese SPEKE v2.0-Spezifikation basiert.
- DASH-IF-System — Die Liste der registrierten Identifikatoren für DRM-Systeme. IDs
- https://github.com/awslabs/speke-reference-server— Beispiel für einen Referenzschlüsselanbieter, den Sie mit Ihrem AWS-Konto verwenden können, um Ihnen den Einstieg in eine SPEKE-Implementierung in AWS zu erleichtern.

Terminologie

Die folgende Liste definiert die in dieser Spezifikation verwendete Terminologie. Sofern möglich, folgt diese Spezifikation der in der DASH-IF CPIX-Spezifikationverwendeten Terminologie.

- ARN — Name der Amazon-Ressource. Eindeutige Bezeichnung einer AWS-Ressource.
- Inhaltsschlüssel — Ein kryptografischer Schlüssel, der zum Verschlüsseln eines Teils des Inhalts verwendet wird.
- Inhaltsanbieter — Ein Herausgeber, der die Rechte und Regeln für die Bereitstellung geschützter Medien bereitstellt. Der Inhaltsanbieter kann auch Quellmedien (Mezzanine-Format, für die

Transcodierung), Asset-IDs, Schlüsselkennungen (KIDs), Schlüsselwerte, Kodierungsanweisungen und Metadaten zur Inhaltsbeschreibung bereitstellen.

- DRM — Verwaltung digitaler Rechte. Wird verwendet, um urheberrechtlich geschützte digitale Inhalte vor nicht genehmigtem Zugriff zu schützen.
- DRM-Plattform — Ein System, das DRM-Funktionen und Unterstützung für Inhaltsverschlüsseler und -betrachter bereitstellt, einschließlich der Bereitstellung von DRM-Schlüsseln und der Lizenzierung für die Verschlüsselung und Entschlüsselung von Inhalten.
- DRM-Anbieter — siehe DRM-Plattform.
- DRM-System — Ein Standard für DRM-Implementierungen. Zu den gängigen DRM-Systemen gehören Apple FairPlay, Google Widevine und Microsoft. PlayReady DRM-Systeme werden von Inhaltsanbietern verwendet, um digitale Inhalte für die Bereitstellung an Betrachter und für den Zugriff durch Betrachter zu schützen. Eine Liste der DRM-Systeme, die bei DASH-IF registriert sind, finden Sie unter DASH-IF-System. IDs Die DASH-IF CPIX-Spezifikation verwendet den hier definierten Begriff „DRM-System“ und an einigen Stellen „DRM-System“, in derselben Bedeutung wie die in diese Spezifikation verwendete Bezeichnung „DRM-Plattform“.
- DRM-Lösung — siehe DRM-Plattform.
- DRM-Technologie — siehe DRM-System.
- Encryptor — Eine Medienverarbeitungskomponente, die Medieninhalte mithilfe von Schlüsseln verschlüsselt, die vom Schlüsselanbieter bezogen wurden. Verschlüsseler fügen den Medien in der Regel auch DRM-Verschlüsselungssignale und Metadaten hinzu. Verschlüsseler sind in der Regel Encoder, Packager und Transcoder.
- Schlüsselanbieter — Die Komponente einer DRM-Plattform, die eine SPEKE-REST-API zur Bearbeitung von Schlüsselanfragen bereitstellt. Der Schlüsselanbieter kann der Schlüsselserver selbst oder eine andere Komponente der Plattform sein.
- Schlüsselserver — Die Komponente einer DRM-Plattform, die Schlüssel für die Verschlüsselung und Entschlüsselung von Inhalten verwaltet.
- Betreiber — Eine Person, die für den Betrieb des Gesamtsystems, einschließlich des Verschlüsselers und des Schlüsselanbieters, verantwortlich ist.
- Player — Ein Mediaplayer, der im Auftrag eines Zuschauers arbeitet. Dieser ruft Informationen aus verschiedenen Quellen ab, darunter Medienmanifestdateien, Mediendateien und DRM-Lizenzen. Fordert für die Betrachter-Lizenzen vom DRM-Server an.

Kunden-Onboarding für SPEKE

Schützen Sie Ihre Inhalte vor unbefugter Nutzung, indem Sie einen DRM-Schlüsselanbieter (Secure Packager und Encoder Key Exchange) mit Ihrem Verschlüsseler und Ihren Media Playern kombinieren. SPEKE definiert den Standard für die Kommunikation zwischen Verschlüsselern und Paketierern von Medieninhalten und Schlüsselanbietern für die Verwaltung digitaler Rechte (DRM). Zum Einrichten wählen Sie einen DRM-Plattformschlüsselanbieter aus und konfigurieren die Kommunikation zwischen dem Schlüsselanbieter und Ihren Verschlüsselern und Playern.

Themen

- Beginnen Sie mit einem DRM-Plattformanbieter
- SPEKE-Support für AWS-Services und -Produkte
- SPEKE-Support für Services und Produkte von AWS-Partnern

Beginnen Sie mit einem DRM-Plattformanbieter

Die folgenden Amazon-Partner bieten DRM-Plattformimplementierungen für SPEKE von Drittanbietern an. Um Details zu den Angeboten und Informationen über die Kontaktaufnahme zu erhalten, klicken Sie auf die Links zu ihren Amazon Partner Network-Seiten. Partner, die keinen Link haben, haben derzeit keine Amazon Partner Network-Seite, aber Sie können sie direkt kontaktieren. Die Partner können Ihnen bei der Einrichtung ihrer Plattformen helfen.

Anbieter der DRM-Plattform	SPEKE v1-Unterstützung	SPEKE v2-Unterstützung
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
DOVERRUNNER	√	√
Insys Cloud-DRM	√	√

Anbieter der DRM-Plattform	SPEKE v1-Unterstützung	SPEKE v2-Unterstützung
Intertrust Technologies	√	√
Irdeto	√	√
JW-Spieler	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKE-Support für AWS-Services und -Produkte

In diesem Abschnitt wird die SPEKE-Unterstützung von AWS Media Services aufgeführt, die in der AWS Cloud und von lokalen AWS-Medienprodukten ausgeführt werden. Diese Services und Produkte sind die Verschlüsseler in der SPEKE-Inhaltsverschlüsselungsarchitektur. Überprüfen Sie, ob Ihr Streaming-Protokoll und das gewünschte DRM-System für Ihren Service oder Ihr Produkt verfügbar sind.

AWS-Service oder -Produkt	SPEKE v1-Unterstützung	SPEKE v2-Unterstützung	Unterstützte DRM-Technologien
AWS Elemental MediaConvert — Service, der in der AWS-Cloud ausgeführt wird	√	√	Dokumentation

AWS-Service oder -Produkt	SPEKE v1-Unterstützung	SPEKE v2-Unterstützung	Unterstützte DRM-Technologien
AWS Elemental MediaPackage — Service, der in der AWS-Cloud ausgeführt wird	√	√	Dokumentation
AWS Elemental Live — Lokales Produkt	√		Dokumentation: MPEG-DASH//HLS
AWS Elemental Server — Lokales Produkt	√		Dokumentation

SPEKE-Support für Services und Produkte von AWS-Partnern

In diesem Abschnitt wird der SPEKE-Support aufgeführt, der von AWS-Partnerservices und -produkten bereitgestellt wird, die in der AWS-Cloud ausgeführt werden. Diese Services und Produkte sind die Verschlüsseler in der SPEKE-Inhaltsverschlüsselungsarchitektur. Überprüfen Sie, ob Ihr Streaming-Protokoll und das gewünschte DRM-System für Ihren Service oder Ihr Produkt verfügbar sind.

AWS-Service oder -Produkt	SPEKE v1-Unterstützung	SPEKE v2-Unterstützung	Unterstützte DRM-Technologien
Bitmovin Live-Videokodierung	√		Dokumentation
Bitmovin Video-on-Demand (VOD) - Codierung	√		Dokumentation

SPEKE API-Spezifikation

Dies ist die REST-API-Spezifikation für Secure Packager and Encoder Key Exchange (SPEKE). Mit dieser Spezifizierung stellen Sie Kunden, die Verschlüsselung verwenden, DRM-Urheberrechtsschutz bereit.

In einem Videostreaming-Workflow kommuniziert die Verschlüsselungs-Engine mit dem Schlüsselanbieter der DRM-Plattform, um Inhaltsschlüssel anzufordern. Diese Schlüssel sind hoch vertraulich. Daher ist es von kritischer Bedeutung, dass Schlüsselanbieter und Verschlüsselungs-Engine einen hochsicheren und vertrauenswürdigen Kommunikationskanal einrichten. Sie können auch die Inhaltsschlüssel im Dokument verschlüsseln, um eine sicherere Verschlüsselung zu gewährleisten. end-to-end

Diese Spezifikation hat folgende Ziele:

- Definieren Sie eine einfache, vertrauenswürdige und hochsichere Schnittstelle, die DRM-Anbieter und -Kunden für die Integration mit Verschlüsselern verwenden können, wenn eine Inhaltsverschlüsselung erforderlich ist.
- Decken Sie VOD- sowie Live-Workflows ab und schließen Sie die Fehlerbedingungen und Authentifizierungsmechanismen ein, die für eine robuste und hochsichere Kommunikation zwischen Verschlüsselern und DRM-Schlüsselanbieter-Endpunkten erforderlich sind.
- Beinhaltet Unterstützung für HLS-, MSS- und DASH-Pakete und ihre gängigen DRM-Systeme: FairPlay,, PlayReady und Widevine/CENC.
- Einfachheit und Erweiterbarkeit der Spezifikation, um zukünftige DRM-Systeme unterstützen zu können.
- Verwendung einer einfachen REST API.

> **Note**
>
>

GARANTIE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF GARANTIEN DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND NICHTVERLETZUNG VON RECHTEN DRITTER. IN KEINEM FALL HAFTEN DIE AUTOREN ODER URHEBERRECHTSINHABER DIESES MATERIALS FÜR ANSPRÜCHE, SCHÄDEN ODER ANDERE VERBINDLICHKEITEN, SEI ES AUS VERTRAG, UNERLAUBTER HANDLUNG ODER AUF ANDERE WEISE, DIE SICH AUS, AUS ODER IN VERBINDUNG MIT DIESEM MATERIAL ODER DER VERWENDUNG ODER ANDEREN GESCHÄFTEN MIT DIESEM MATERIAL ERGEBEN.

Themen

- Für SPEKE ist eine Authentifizierung erforderlich
- SPEKE API v1
- SPEKE API v2
- Lizenz für die SPEKE API-Spezifikation

Für SPEKE ist eine Authentifizierung erforderlich

SPEKE erfordert eine Authentifizierung für lokale Produkte sowie für Dienste und Funktionen, die in der AWS-Cloud ausgeführt werden.

Themen

- Authentifizierung für AWS-Cloud-Implementierungen
- Authentifizierung für lokale Produkte

Authentifizierung für AWS-Cloud-Implementierungen

SPEKE benötigt für die Verwendung mit einem Verschlüsseler eine AWS-Authentifizierung über IAM-Rollen. IAM-Rollen werden vom DRM-Anbieter oder dem Operator erstellt, der im Besitz des DRM-Endpunkts in einem AWS-Konto ist. Jeder Rolle ist ein Amazon-Ressourcenname (ARN) zugewiesen, den der AWS Elemental-Service-Operator in der Service-Konsole angibt, wenn er Verschlüsselung anfordert. Die Richtlinienberechtigungen der Rolle müssen so konfiguriert werden, dass sie zum Zugriff auf die Schlüsselanbieter-API berechtigen, nicht jedoch auf andere AWS-Ressourcen. Wenn der Verschlüsseler Kontakt mit dem DRM-Schlüsselanbieter aufnimmt, verwendet er den Rollen-ARN, um die Rolle des Kontoinhabers des Schlüsselanbieters anzunehmen.

Anschließend werden temporäre Anmeldeinformationen an den Verschlüsseler zurückgegeben, mit denen dieser auf den Schlüsselanbieter zugreifen kann.

Eine gängige Implementierung besteht darin, dass der Betreiber oder DRM-Plattformanbieter Amazon API Gateway vor dem Schlüsselanbieter verwendet und dann die AWS Identity and Access Management (AWS IAM) -Autorisierung für die API Gateway-Ressource aktiviert. Sie können das folgende Beispiel für eine Richtliniendefinition einer neuen Rolle anfügen, um der entsprechenden Ressource Berechtigungen zu erteilen. In diesem Fall gelten die Berechtigungen für alle API-Gateway-Ressourcen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "execute-api:Invoke"
            ],
            "Resource": [
                "arn:aws:execute-api:us-west-2:*:*/*/GET/*"
            ]
        }
    ]
}
```

Schließlich erfordert die Rolle das Hinzufügen einer Vertrauensstellung und der Operator muss den Service auswählen können.

Das folgende Beispiel zeigt einen Rollen-ARN, der für den Zugriff auf den DRM-Schlüsselanbieter erstellt wurde:

```
arn:aws:iam::2949266363526:role/DRMKeyServer
```

Weitere Informationen zur Erstellung einer Rolle finden Sie unter AWS AssumeRole. Weitere Informationen zum Signieren einer Anforderung finden Sie unter AWS Sigv4.

Authentifizierung für lokale Produkte

Für lokale Produkte empfehlen wir die Verwendung von SSL/TLS und Digest-Authentifizierung, um die beste Sicherheit zu erzielen. Sie sollten jedoch mindestens die grundlegende Authentifizierung über HTTPS verwenden.

Beide Arten der Authentifizierung verwenden den Header `Authorization` in der HTTP-Anforderung:

- Digest-Authentifizierung — Der Autorisierungsheader besteht aus der Kennung, `Digest` gefolgt von einer Reihe von Werten, die die Anfrage authentifizieren. Insbesondere wird ein Antwortwert durch eine Reihe von MD5 Hashfunktionen generiert, zu denen eine eindeutige one-time-use Nonce vom Server gehört, mit der sichergestellt wird, dass das Passwort sicher übertragen wird.
- Standardauthentifizierung — Der Autorisierungsheader besteht aus der Kennung, `Basic` gefolgt von einer Base-64-kodierten Zeichenfolge, die den Benutzernamen und das Passwort darstellt, getrennt durch einen Doppelpunkt.

Informationen zur Basis- und Digest-Authentifizierung einschließlich detailliertet Informationen zum Header finden Sie in der Internet Engineering Task Force (IETF)-Spezifikation RFC 2617 – HTTP-Authentifizierung: Basis- und Digest-Zugriffsauthentifizierung.

SPEKE API v1

Dies ist die REST-API für Secure Packager und Encoder Key Exchange (SPEKE) v1. Mit dieser Spezifizierung stellen Sie Kunden, die Verschlüsselung verwenden, DRM-Urheberrechtsschutz bereit. Um SPEKE-konform zu sein, muss Ihr DRM-Schlüsselanbieter die in dieser Spezifikation beschriebene REST-API verfügbar machen. Der Verschlüsseler führt API-Aufrufe Ihres Schlüsselanbieters durch.

> **Note**
>
> Die Codebeispiele in dieser Spezifikation dienen lediglich der Illustration. Sie können die Beispiele nicht ausführen, da sie nicht Teil einer vollständigen SPEKE-Implementierung sind.

SPEKE verwendet die Datenstrukturdefinition des DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) für den Schlüsselaustausch, mit einigen Einschränkungen. DASH-IF-CPIXdefiniert ein Schema, das einen erweiterbaren Multi-DRM-Austausch von der DRM-Plattform zum Verschlüsseler ermöglicht. So wird für alle Verpackungsformate mit adaptiven Bitraten zum Zeitpunkt der Inhaltkompression und -verpackung Inhaltsverschlüsselung bereitgestellt. Zu den Verpackungsformaten mit adaptiven Bitraten gehören HLS, DASH und MSS.

Ausführliche Informationen zum Austauschformat finden Sie in der CPIX-Spezifikation des DASH Industry Forum unter https://dashif. org/docs/DASH-IF-CPIX-v2-0.pdf.

Themen

- SPEKE API v1 — Anpassungen und Einschränkungen der DASH-IF-Spezifikation
- SPEKE API v1 — Standard-Payload-Komponenten
- SPEKE API v1 — Beispiele für Live-Workflow-Methodenaufrufe
- SPEKE API v1 — Beispiele für VOD-Workflow-Methodenaufrufe
- SPEKE API v1 — Inhaltsschlüsselverschlüsselung
- SPEKE API v1 — Heartbeat
- SPEKE API v1 — Überschreiben der Schlüssel-ID

SPEKE API v1 — Anpassungen und Einschränkungen der DASH-IF-Spezifikation

Die DASH-IF CPIX-Spezifikation, https://dashif. org/docs/DASH-IF-CPIX-v2-0.pdf unterstützt eine Reihe von Anwendungsfällen und Topologien. Die SPEKE-API-Spezifikation entspricht der CPIX-Spezifikation mit den folgenden Anpassungen und Einschränkungen:

- SPEKE folgt dem Encryptor Consumer-Workflow.
- Für verschlüsselte Inhaltsschlüssel wendet SPEKE die folgenden Einschränkungen an:
  - SPEKE unterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
  - SPEKE benötigt 2048 RSA-basierte Zertifikate.
- Für rotierende wichtige Workflows benötigt SPEKE den Filter,. `ContentKeyUsageRule` `KeyPeriodFilter` SPEKE ignoriert alle anderen Einstellungen. `ContentKeyUsageRule`
- SPEKE lässt die Funktionalität weg. `UpdateHistoryItemList` Wenn die Liste in der Antwort vorhanden ist, ignoriert SPEKE sie.
- SPEKE unterstützt die Schlüsselrotation. SPEKE verwendet nur `ContentKeyPeriod@index, um den Schlüsselzeitraum zu verfolgen.
- Um MSS zu unterstützen PlayReady, verwendet SPEKE einen benutzerdefinierten Parameter unter dem `DRMSystem` Tag,. `SPEKE:ProtectionHeader`

- Wenn bei einer HLS-Verpackung `URIExtXKey` in der Antwort enthalten ist, muss sie die vollständigen Daten enthalten, die dem URI-Parameter des Tag `EXT-X-KEY` einer HLS-Wiedergabeliste ohne weitere Signalisierungsanforderung hinzugefügt werden sollen.
- Für die HLS-Playlist stellt SPEKE unter dem `DRMSystem` Tag die optionalen benutzerdefinierten Parameter `speke:KeyFormat` und `speke:KeyFormatVersions` für die Werte des Tags `KEYFORMAT` und die `KEYFORMATVERSIONS` Parameter des Tags bereit. `EXT-X-KEY`

  Der HLS-Initialisierungsvektor (IV) folgt stets der Segmentnummer, es sei denn, dies wird vom Operator ausdrücklich anders festgelegt.
- Beim Anfordern von Schlüsseln verwendet der Verschlüsseler möglicherweise das optionale Attribut `@explicitIV` des Elements `ContentKey`. Der Schlüsselanbieter kann mit einem IV unter Verwendung von `@explicitIV` antworten, auch wenn das Attribut nicht in der Anforderung enthalten ist.
- Die Verschlüsseler erstellt die Schlüssel-ID (`KID`), die für alle Inhalts-IDs und Schlüsselzeiträume gleich bleibt. Der Schlüsselanbieter schließt `KID` in seiner Antwort auf das Anforderungsdokument ein.
- Der Schlüsselanbieter enthält möglicherweise einen Wert für den `Speke-User-Agent`-Antwort-Header, um sich zu Debugging-Zwecken zu identifizieren.
- SPEKE unterstützt derzeit nicht mehrere Titel oder Keys pro Inhalt.

  Der SPEKE-konforme Verschlüsseler fungiert als Client und sendet `POST` Operationen an den Endpunkt des Schlüsselanbieters. Der Verschlüsseler sendet möglicherweise eine regelmäßige `heartbeat`-Anforderung, um sicherzustellen, dass die Verbindung zwischen dem Verschlüsseler und dem Schlüsselanbieter-Endpunkt stabil ist.

SPEKE API v1 — Standard-Payload-Komponenten

Der Verschlüsseler kann in allen SPEKE-Anforderungen Antworten für mindestens ein DRM-System anfordern. Der Verschlüsseler gibt die DRM-Systeme in `<cpix:DRMSystemList>` der Anforderungsnutzlast an. Jede Systemspezifikation enthält den Schlüssel und gibt den Typ der zurückzugebenden Antwort an.

Das folgende Beispiel zeigt eine DRM-Systemliste mit einer einzigen DRM-Systemspezifikation:

```
<cpix:DRMSystemList>
    <!--HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    systemId="81376844-f976-481e-a84e-cc25d39b0b33">
        <cpix:URIExtXKey></cpix:URIExtXKey>
        <speke:KeyFormat></speke:KeyFormat>
        <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>
</cpix:DRMSystemList>
```

In der folgenden Tabelle werden die Hauptkomponenten für jedes `<cpix:DRMSystem>` aufgelistet.

Kennung	Beschreibung
`systemId` oder `schemeId`	Eindeutige ID für den Typ des DRM-Systems wie bei der DASH-IF-Organisation registriert. Eine Liste finden Sie unter DASH-IF System. IDs
`kid`	Die Schlüssel-ID. Dies ist nicht der eigentliche Schlüssel, sondern eine ID, die in einer Hash-Tabelle auf den Schlüssel verweist.
`<cpix:UriExtXKey>`	Fordert einen unverschlüsselten Standards chlüssel an. Der Schlüsselantworttyp muss entweder diese oder die PSSH-Antwort sein.
`<cpix:PSSH>`	Fordert einen Protection System Specific Header (PSSH) an. Diese Art von Header enthält einen Verweis auf die `kid`, die `systemID` und benutzerdefinierte Daten für den DRM-Anbieter als Teil von Common Encryption (CENC). Der Schlüsselantworttyp muss entweder diese oder die `UriExtXKey` -Antwort sein.

_Beispielanfragen für Standardschlüssel und für PSSH _

Das folgende Beispiel zeigt einen Teil einer Beispielanforderung des Verschlüsselers an den DRM-Schlüsselanbieter. Die Hauptkomponenten sind hervorgehoben. Die erste Anforderung bezieht sich auf einen Standardschlüssel. Die zweite Anforderung bezieht sich auf eine PSSH-Antwort:

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc" xmlns:speke="urn:aws:amazon:com:speke">
    <cpix:ContentKeyList>
        <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
        explicitIV="OFj2IjCsPJFfMAxmQxLGPw==></cpix:ContentKey>
    </cpix:ContentKeyList>
    <cpix:DRMSystemList>
        <!-- HLS AES-128 (systemId is implementation specific)-->
        <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
        systemId="81376844-f976-481e-a84e-cc25d39b0b33"> ← System Id
            <cpix:URIExtXKey></cpix:URIExtXKey> ← request Key
            <speke:KeyFormat></speke:KeyFormat>
            <speke:KeyFormatVersions></speke:KeyFormatVersions>
        </cpix:DRMSystem>

        <!-- Common encryption (Widevine)-->
        <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
        systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed"> ← System Id
            <cpix:PSSH></cpix:PSSH> ← request PSSH
        </cpix:DRMSystem>

    </cpix:DRMSystemList>
    ...
</cpix:CPIX>
```

_Beispielantworten für Standard Key und für PSSH _

Das folgende Beispiel zeigt die entsprechende Antwort des DRM-Schlüsselanbieters für den Verschlüsseler:

```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix" xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
    <cpix:ContentKeyList>
        <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
        kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
            <cpix:Data>
                <pskc:Secret>
                    <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
                </pskc:Secret>
            </cpix:Data>
        </cpix:ContentKey>
    </cpix:ContentKeyList>
    <cpix:DRMSystemList>
        <!-- HLS AES-128 (systemId is implementation specific) -->
        <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"  <-- KID
        systemId="81376844-f976-481e-a84e-cc25d39b0b33">  <-- System Id

            <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3M
            uY29tL0VrZVN0YWdlL2NsaWVudC9hYmMxMjMvOThlZTU1OTYtY2QzZS1hMjBkLTE2M2EtZTM4MjQyMGM2ZWZ
            m</cpix:URIExtXKey>  <-- Key
            <speke:KeyFormat>aWRlbnRpdHk=</speke:KeyFormat>
            <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
        </cpix:DRMSystem>

        <!-- Common encryption (Widevine) -->
        <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"  <-- KID
        systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">  <-- System Id

            <cpix:PSSH>AAAAanBzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd
            2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOYmI3RGppNnNBdEtaelE9PSoCU0QyAA==</cpix:PSSH>  <-- PSSH
        </cpix:DRMSystem>

    </cpix:DRMSystemList>
    ...
</cpix:CPIX>
```

SPEKE API v1 — Beispiele für Live-Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Die folgende URL ist lediglich ein Beispiel und gibt kein bestimmtes Format vor:

```
POST https://speke-compatible-server/speke/v1.0/copyProtection
```

Anforderungstext

Ein CPIX-Element.

Anforderungs-Header

Name	Typ	Auftreten	Beschreibung
`AWS Authorization`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`X-Amz-Security-Token`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`X-Amz-Date`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`Content-Type`	String	1..1	application/xml

Antwort-Header

Name	Typ	Auftreten	Beschreibung
`Speke-User-Agent`	String	1..1	Zeichenfolge, die den Schlüsselanbieter identifiziert.
`Content-Type`	String	1..1	application/xml

Request Response (Antwort anfordern)

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`200 (Success)`	CPIX	1..1	DASH-CPIX-Nutzlast antwort
`4XX (Client error)`	Client-Fehlermeldung	1..1	Beschreibung des Client-Fehlers.

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`5XX (Server error)`	Server-Fehlermeldung	1..1	Beschreibung des Server-Fehlers.

> **Note**
>
> Die Beispiele in diesem Abschnitt zeigen keine Inhaltsschlüssel-Verschlüsselung. Informationen zum Hinzufügen von Inhaltsschlüsselverschlüsselung finden Sie unter Inhaltsschlüsselverschlüsselung.

Beispiel für eine Live-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Live-Anforderungsnutzlast vom Verschlüsseler an den DRM-Schlüsselanbieter:

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
 xmlns:speke="urn:aws:amazon:com:speke">
 <cpix:ContentKeyList>
  <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 explicitIV="OFj2IjCsPJFfMAxmQxLGPw==></cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">
   <cpix:URIExtXKey></cpix:URIExtXKey>
   <speke:KeyFormat></speke:KeyFormat>
   <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- HLS SAMPLE-AES -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:URIExtXKey></cpix:URIExtXKey>
   <speke:KeyFormat></speke:KeyFormat>
   <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>
```

```
  <!-- Common encryption (Widevine)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>

  <!-- Common encryption / MSS (Playready) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <speke:ProtectionHeader></speke:ProtectionHeader>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Beispiel für eine Live-Antwortnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Antwortnutzlast des DRM-Schlüsselanbieters:

```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
 xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific) -->
```

```
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">

 <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIExtXKey>
   <speke:KeyFormat>aWRlbnRpdHk=</speke:KeyFormat>
   <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- HLS SAMPLE-AES -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

 <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIExtXKey>
   <speke:KeyFormat>Y29tLmFwcGxlLnN0cmVhbWluZ2tleWRlbGl2ZXJ5</speke:KeyFormat>
   <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- Common encryption (Widevine) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOY
cpix:PSSH>
  </cpix:DRMSystem>

  <!-- Common encryption / MSS (Playready) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">

 <speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAiAGgAdAB0AH
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEkARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQ
+AGgAdAB0AHAAOgAvAC8AcABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgBlAGMAdAB0AGEAcABzAC4AbgBlAHQALwBwAHIALw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

 <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4IhflQAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAcA
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
```

```
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v1 — Beispiele für VOD-Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Die folgende URL ist lediglich ein Beispiel und gibt kein bestimmtes Format vor.

```
POST https://speke-compatible-server/speke/v1.0/copyProtection
```

Anforderungstext

Ein CPIX-Element.

Antwort-Header

Name	Typ	Auftreten	Beschreibung
`Speke-User-Agent`	String	1..1	Zeichenfolge, die den Schlüsselanbieter identifiziert.
`Content-Type`	String	1..1	application/xml

Request Response (Antwort anfordern)

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`200 (Success)`	CPIX	1..1	DASH-CPIX-Nutzlast antwort

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`4XX (Client error)`	Client-Fehlermeldung	1..1	Beschreibung des Client-Fehlers.
`5XX (Server error)`	Server-Fehlermeldung	1..1	Beschreibung des Server-Fehlers.

> **Note**
>
> Die Beispiele in diesem Abschnitt zeigen keine Inhaltsschlüssel-Verschlüsselung. Informationen zum Hinzufügen von Inhaltsschlüsselverschlüsselung finden Sie unter Inhaltsschlüsselverschlüsselung.

Beispiel für eine VOD-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine grundlegende VOD-Anforderungsnutzlast vom Verschlüsseler an den DRM-Schlüsselanbieter:

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
 xmlns:speke="urn:aws:amazon:com:speke">
 <cpix:ContentKeyList>
  <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 explicitIV="OFj2IjCsPJFfMAxmQxLGPw==></cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">
   <cpix:URIExtXKey></cpix:URIExtXKey>
   <speke:KeyFormat></speke:KeyFormat>
   <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- HLS SAMPLE-AES -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:URIExtXKey></cpix:URIExtXKey>
```

```
   <speke:KeyFormat></speke:KeyFormat>
   <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- Common encryption (Widevine)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>

  <!-- Common encryption / MSS (Playready) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <speke:ProtectionHeader></speke:ProtectionHeader>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
    </cpix:CPIX>
```

Beispiel für eine VOD-Antwortnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine grundlegende VOD-Antwortnutzlast des DRM-Schlüsselanbieters:

```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
 xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">

 <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIExtXKey>
   <speke:KeyFormat>aWRlbnRpdHk=</speke:KeyFormat>
```

```
   <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- HLS SAMPLE-AES -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

 <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIExtXKey>
   <speke:KeyFormat>Y29tLmFwcGxlLnN0cmVhbWluZ2tleWRlbGl2ZXJ5</speke:KeyFormat>
   <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- Common encryption (Widevine) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOY
cpix:PSSH>
  </cpix:DRMSystem>

  <!-- Common encryption / MSS (Playready) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">

 <speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAiAGgAdAB0AH
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEkARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQ
+AGgAdAB0AHAAOgAvAC8AcABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgBlAGMAdAB0AGEAcABzAC4AbgBlAHQALwBwAHIALw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

 <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4IhflQAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAcA
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
</cpix:CPIX>
```

SPEKE API v1 — Inhaltsschlüsselverschlüsselung

Sie können Ihrer SPEKE-Implementierung optional eine Inhaltsschlüsselverschlüsselung hinzufügen. Die Inhaltsschlüsselverschlüsselung garantiert vollständigen end-to-end Schutz, indem sie zusätzlich zur Verschlüsselung des Inhalts selbst auch die Inhaltsschlüssel für die Übertragung verschlüsselt. Wenn Sie dies nicht für Ihren Schlüsselanbieter implementieren, verlassen Sie sich aus Sicherheitsgründen auf die Verschlüsselung der Transportschicht sowie auf eine starke Authentifizierung.

Um die Inhaltsschlüsselverschlüsselung für Verschlüsseler zu verwenden, die in der AWS-Cloud ausgeführt werden, importieren Kunden Zertifikate in den AWS Certificate Manager und verwenden das resultierende Zertifikat dann ARNs für ihre Verschlüsselungsaktivitäten. Der Verschlüsseler verwendet das Zertifikat ARNs und den ACM-Service, um verschlüsselte Inhaltsschlüssel für den DRM-Schlüsselanbieter bereitzustellen.

Einschränkungen

SPEKE unterstützt die Verschlüsselung von Inhaltsschlüsseln gemäß der DASH-IF CPIX-Spezifikation mit den folgenden Einschränkungen:

- SPEKE unterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
- SPEKE benötigt 2048 RSA-basierte Zertifikate.

Diese Einschränkungen sind auch unter Anpassungen und Einschränkungen der DASH-IF-Spezifikation aufgeführt.

Implementieren der Inhaltsschlüssel-Verschlüsselung

Um Inhaltsschlüssel-Verschlüsselung bereitzustellen, führen Sie in den Implementierungen Ihres DRM-Schlüsselanbieters Folgendes aus:

- Verarbeiten Sie das Element `<cpix:DeliveryDataList>` in den Anforderungs- und Antwortnutzlasten.
- Stellen Sie in der `<cpix:ContentKeyList>` der Antwortnutzlasten verschlüsselte Werte bereit.

Weitere Informationen zu diesen Elementen finden Sie in der DASH-IF CPIX 2.0-Spezifikation.

Beispiel für das Inhaltsschlüssel-Verschlüsselungselement `<cpix:DeliveryDataList>` in der Anforderungsnutzlast

Im folgenden Beispiel wird das hinzugefügte `<cpix:DeliveryDataList>`-Element in Fettschrift hervorgehoben:

```
<?xml version="1.0" encoding="UTF-8"?>
<cpix:CPIX id="example-test-doc-encryption"
    xmlns:cpix="urn:dashif:org:cpix"
    xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
    xmlns:speke="urn:aws:amazon:com:speke">
    <cpix:DeliveryDataList>
        <cpix:DeliveryData id="<ORIGIN SERVER ID>">
            <cpix:DeliveryKey>
                <ds:X509Data>
                    <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
                </ds:X509Data>
            </cpix:DeliveryKey>
        </cpix:DeliveryData>
    </cpix:DeliveryDataList>
    <cpix:ContentKeyList>
     ...
    </cpix:ContentKeyList>
</cpix:CPIX>
```

Beispiel für das Inhaltsschlüssel-Verschlüsselungselement `<cpix:DeliveryDataList>` in der Antwortnutzlast

Im folgenden Beispiel wird das hinzugefügte `<cpix:DeliveryDataList>`-Element in Fettschrift hervorgehoben:

```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
    xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
    xmlns:speke="urn:aws:amazon:com:speke" id="hls_test_001">
    <cpix:DeliveryDataList>
        <cpix:DeliveryData id="<ORIGIN SERVER ID>">
            <cpix:DeliveryKey>
                <ds:X509Data>
                    <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
                </ds:X509Data>
```

```
            </cpix:DeliveryKey>
            <cpix:DocumentKey Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc">
                <cpix:Data>
                    <pskc:Secret>
                        <pskc:EncryptedValue>
                            <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                            <enc:CipherData>
                                <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                            </enc:CipherData>
                        </pskc:EncryptedValue>
                        <pskc:ValueMAC>qnei/5TsfUwDu+8bhsZrLjDRDngvmnUZD2eva7SfXWw=</
pskc:ValueMAC>
                    </pskc:Secret>
                </cpix:Data>
            </cpix:DocumentKey>
            <cpix:MACMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-
sha512">
                <cpix:Key>
                    <pskc:EncryptedValue>
                        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                        <enc:CipherData>
                            <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                        </enc:CipherData>
                    </pskc:EncryptedValue>
                    <pskc:ValueMAC>DGqdpHUfFKxdsO9+EWrPjtdTCVfjPLwwtzEcFC/j0xY=</
pskc:ValueMAC>
                </cpix:Key>
            </cpix:MACMethod>
        </cpix:DeliveryData>
    </cpix:DeliveryDataList>
    <cpix:ContentKeyList>
     ...
    </cpix:ContentKeyList>
</cpix:CPIX>
```

Beispiel für das Inhaltsschlüssel-Verschlüsselungselement `<cpix:ContentKeyList>` in der Antwortnutzlast

Das folgende Beispiel zeigt die Behandlung des verschlüsselten Inhaltsschlüssels im `<cpix:ContentKeyList>`-Element der Antwortnutzlast. Hier wird das Element `<pskc:EncryptedValue>` verwendet:

```
   <cpix:ContentKeyList>
        <cpix:ContentKey kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
            <cpix:Data>
                <pskc:Secret>
                    <pskc:EncryptedValue>
                        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
                        <enc:CipherData>
                            <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
                        </enc:CipherData>
                    </pskc:EncryptedValue>
                    <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
                </pskc:Secret>
            </cpix:Data>
        </cpix:ContentKey>
    </cpix:ContentKeyList>
```

Im Vergleich dazu zeigt das folgende Beispiel eine ähnliche Antwortnutzlast mit dem unverschlüsselten Inhaltsschlüssel als entschlüsselter Schlüssel. Hier wird das Element `<pskc:PlainValue>` verwendet:

```
    <cpix:ContentKeyList>
        <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
 kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
            <cpix:Data>
                <pskc:Secret>
                    <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
                </pskc:Secret>
            </cpix:Data>
        </cpix:ContentKey>
    </cpix:ContentKeyList>
```

SPEKE API v1 — Heartbeat

Beispiel für eine Anforderungssyntax

Die folgende URL ist lediglich ein Beispiel und gibt kein bestimmtes Format vor:

```
GET https://speke-compatible-server/speke/v1.0/heartbeat
```

Request Response (Antwort anfordern)

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`200 (Success)`	Statusmeldung	1..1	Eine Nachricht, die den Status beschreibt.

SPEKE API v1 — Überschreiben der Schlüssel-ID

Der Verschlüsseler erstellt bei jeder Rotation der Schlüssel eine neue Schlüssel-ID (Key Identifier, KID). Er übergibt die KID an den DRM-Schlüsselanbieter bei dessen Anforderungen. Beinahe immer antwortet der Schlüsselanbieter mit derselben KID. Er kann jedoch in der Antwort auch einen anderen Wert für die KID bereitstellen.

Im Folgenden finden Sie eine Beispielanforderung mit der KID `11111111-1111-1111-1111-111111111111`:

```
   <cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke">
     <cpix:ContentKeyList>
      <cpix:ContentKey kid="11111111-1111-1111-1111-111111111111"></cpix:ContentKey>
     </cpix:ContentKeyList>
     <cpix:DRMSystemList>
      <!-- Common encryption (Widevine)-->
      <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
       <cpix:PSSH />
      </cpix:DRMSystem>
     </cpix:DRMSystemList>
     <cpix:ContentKeyPeriodList>
      <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
     </cpix:ContentKeyPeriodList>
     <cpix:ContentKeyUsageRuleList>
      <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111">
       <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
      </cpix:ContentKeyUsageRule>
     </cpix:ContentKeyUsageRuleList>
```

```
    </cpix:CPIX>
```

Die folgende Antwort überschreibt die KID zu 22222222-2222-2222-2222-222222222222:

```
    <cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
 xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
     <cpix:ContentKeyList>
      <cpix:ContentKey explicitIV="ASgwx9pQ2/2lnDzJsUxWcQ=="
 kid="22222222-2222-2222-2222-222222222222">
       <cpix:Data>
        <pskc:Secret>
         <pskc:PlainValue>p3dWaHARtL97MpT7TE916w==</pskc:PlainValue>
        </pskc:Secret>
       </cpix:Data>
      </cpix:ContentKey>
     </cpix:ContentKeyList>
     <cpix:DRMSystemList>
      <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
       <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOY
cpix:PSSH>
      </cpix:DRMSystem>
     </cpix:DRMSystemList>
     <cpix:ContentKeyPeriodList>
      <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
     </cpix:ContentKeyPeriodList>
     <cpix:ContentKeyUsageRuleList>
      <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222">
       <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
      </cpix:ContentKeyUsageRule>
     </cpix:ContentKeyUsageRuleList>
    </cpix:CPIX>
```

SPEKE API v2

Dies ist die REST-API für Secure Packager und Encoder Key Exchange (SPEKE) v2. Mit dieser Spezifizierung stellen Sie Kunden, die Verschlüsselung verwenden, DRM-Urheberrechtsschutz bereit. Um SPEKE-konform zu sein, muss Ihr DRM-Schlüsselanbieter die in dieser Spezifikation

beschriebene REST-API verfügbar machen. Der Verschlüsseler führt API-Aufrufe Ihres Schlüsselanbieters durch.

> **Note**
>
> Die Codebeispiele in dieser Spezifikation dienen lediglich der Illustration. Sie können die Beispiele nicht ausführen, da sie nicht Teil einer vollständigen SPEKE-Implementierung sind.

SPEKE verwendet die Datenstrukturdefinition des DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) für den Schlüsselaustausch, mit einigen Einschränkungen. DASH-IF-CPIXdefiniert ein Schema, das einen erweiterbaren Multi-DRM-Austausch von der DRM-Plattform zum Verschlüsseler ermöglicht. So wird für alle Verpackungsformate mit adaptiven Bitraten zum Zeitpunkt der Inhaltkompression und -verpackung Inhaltsverschlüsselung bereitgestellt. Zu den Verpackungsformaten mit adaptiven Bitraten gehören HLS, DASH und MSS.

Ab der Version 2.0 ist SPEKE auf eine bestimmte CPIX-Version ausgerichtet:

Auf der SPEKE-Seite wird dies durch die Verwendung des `X-Speke-Version` HTTP-Headers und auf der CPIX-Seite durch die Verwendung des Attributs erzwungen. `CPIX@version` Das Fehlen dieser Elemente in den Anfragen ist typisch für ältere SPEKE v1-Workflows. In SPEKE v2-Workflows wird erwartet, dass der Schlüsselanbieter CPIX-Dokumente nur verarbeitet, wenn er beide Versionsparameter unterstützt.

Detaillierte Informationen zum Austauschformat finden Sie in der CPIX 2.3-Spezifikation des DASH Industry Forum.

Insgesamt bringt SPEKE v2.0 im Vergleich zu SPEKE v1.0 die folgenden Weiterentwicklungen:

- Alle Tags aus dem SPEKE-XML-Namespace sind zugunsten gleichwertiger Tags im CPIX-XML-Namespace veraltet
- `SPEKE:ProtectionHeader`ist veraltet und wird ersetzt durch `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`, `SPEKE:KeyFormat` und `SPEKE:KeyFormatVersions` sind veraltet und wurden ersetzt durch `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id`wird ersetzt durch `CPIX@contentId`
- Neue obligatorische CPIX-Attribute:, `CPIX@version` `ContentKey@commonEncryptionScheme`

- Neues optionales CPIX-Element: `DRMSystem.ContentProtectionData`
- Support für mehrere Inhaltsschlüssel
- Versionsübergreifender Mechanismus zwischen SPEKE und CPIX
- Entwicklung der HTTP-Header: neuer Header, Header umbenannt in `X-Speke-Version` `Speke-User-Agent` `X-Speke-User-Agent`
- Veraltete Heartbeat-API

Da die SPEKE v1.0-Spezifikation unverändert bleibt, müssen bestehende Implementierungen nicht geändert werden, um SPEKE v1.0-Workflows weiterhin zu unterstützen.

Themen

- SPEKE API v2 — Anpassungen und Einschränkungen der DASH-IF-Spezifikation
- SPEKE API v2 — Standard-Payload-Komponenten
- SPEKE API v2 - Verschlüsselungsvertrag
- SPEKE API v2 — Beispiele für Live-Workflow-Methodenaufrufe
- SPEKE API v2 — Beispiele für VOD-Workflow-Methodenaufrufe
- SPEKE API v2 — Verschlüsselung von Inhaltsschlüsseln
- SPEKE API v2 — Überschreiben der Schlüssel-ID

SPEKE API v2 — Anpassungen und Einschränkungen der DASH-IF-Spezifikation

Die CPIX 2.3-Spezifikation des DASH Industry Forum unterstützt eine Reihe von Anwendungsfällen und Topologien. Die SPEKE API v2.0-Spezifikation definiert sowohl ein CPIX-Profil als auch eine API für CPIX. Um diese beiden Ziele zu erreichen, hält sie sich an die CPIX-Spezifikation mit den folgenden Anpassungen und Einschränkungen:

CPIX-Profil

- SPEKE folgt dem Encryptor Consumer-Workflow.
- Für verschlüsselte Inhaltsschlüssel wendet SPEKE die folgenden Einschränkungen an:
  - SPEKE unterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
  - SPEKE benötigt 2048 RSA-basierte Zertifikate.

- SPEKE nutzt nur einen Teil der CPIX-Funktionen:
  - SPEKE lässt die Funktionalität weg. `UpdateHistoryItemList` Wenn die Liste in der Antwort vorhanden ist, ignoriert SPEKE sie.
  - SPEKE lässt die Root-/Leaf-Tasten-Funktionalität weg. Wenn das `ContentKey@dependsOnKey` Attribut in der Antwort vorhanden ist, ignoriert SPEKE es.
  - SPEKE lässt das `BitrateFilter` Element und das Attribut weg. `VideoFilter@wcg` Wenn diese Elemente oder Attribute in der CPIX-Nutzlast vorhanden sind, ignoriert SPEKE sie.
- Nur die Elemente oder Attribute, auf die auf der Seite Standard-Payload-Komponenten oder der Seite mit dem Verschlüsselungsvertrag als „Unterstützt“ verwiesen wird, können in CPIX-Dokumenten verwendet werden, die mit SPEKE v2 ausgetauscht werden.
- Wenn sie vom Verschlüsseler in einer CPIX-Anfrage enthalten sind, müssen alle Elemente und Attribute in der CPIX-Antwort des Schlüsselanbieters einen gültigen Wert enthalten. Wenn nicht, stoppt der Verschlüsseler und gibt einen Fehler aus.
- SPEKE unterstützt die Schlüsselrotation mit `KeyPeriodFilter` Elementen. SPEKE verwendet nur die`ContentKeyPeriod@index`, um den Schlüsselzeitraum zu verfolgen.
- Für die HLS-Signalisierung müssen mehrere `DRMSystem.HLSSignalingData` Elemente verwendet werden: eines mit dem `DRMSystem.HLSSignalingData@playlist` Attributwert „media“ und eines mit dem `DRMSystem.HLSSignalingData@playlist` Attributwert „master“.
- Beim Anfordern von Schlüsseln verwendet der Verschlüsseler möglicherweise das optionale Attribut `@explicitIV` des Elements `ContentKey`. Der Schlüsselanbieter kann mit einem IV unter Verwendung von `@explicitIV` antworten, auch wenn das Attribut nicht in der Anforderung enthalten ist.
- Die Verschlüsseler erstellt die Schlüssel-ID (`KID`), die für alle Inhalts-IDs und Schlüsselzeiträume gleich bleibt. Der Schlüsselanbieter schließt `KID` in seiner Antwort auf das Anforderungsdokument ein.
- Der Verschlüsseler muss einen Wert für das Attribut enthalten. `CPIX@contentId` Wenn der Schlüsselanbieter einen leeren Wert für dieses Attribut erhält, gibt er einen Fehler mit der Beschreibung „Missing CPIX @contentId“ zurück. `CPIX@contentId`Der Wert kann vom Schlüsselanbieter nicht überschrieben werden.

  `CPIX@id`Wert, falls nicht Null, muss vom Schlüsselanbieter ignoriert werden.
- Der Verschlüsseler muss einen Wert für das `CPIX@version` Attribut enthalten. Wenn der Schlüsselanbieter einen leeren Wert für dieses Attribut erhält, gibt er einen Fehler mit der Beschreibung „Missing CPIX @version“ zurück. Wenn eine Anfrage mit einer nicht unterstützten

Version empfangen wird, muss die vom Schlüsselanbieter zurückgegebene Fehlerbeschreibung „Unsupported CPIX @version“ lauten.

`CPIX@version`Der Wert kann vom Schlüsselanbieter nicht überschrieben werden.

- Der Verschlüsseler muss für jeden angeforderten Schlüssel einen Wert für das `ContentKey@commonEncryptionScheme` Attribut angeben. Wenn der Schlüsselanbieter einen leeren Wert für dieses Attribut erhält, gibt er einen Fehler mit der Beschreibung „Missing ContentKey @ commonEncryptionScheme for KID`id`“ zurück.

  Ein einzelnes CPIX-Dokument kann nicht mehrere Werte für verschiedene Attribute kombinieren. `ContentKey@commonEncryptionScheme` Beim Empfang einer solchen Kombination gibt der Schlüsselanbieter einen Fehler mit der Beschreibung „Nicht konforme ContentKey @-Kombination“ zurück. commonEncryptionScheme

  Nicht alle `ContentKey@commonEncryptionScheme` Werte sind mit allen DRM-Technologien kompatibel. Beim Empfang einer solchen Kombination gibt der Schlüsselanbieter einen Fehler mit der Beschreibung „ContentKey@ commonEncryptionScheme nicht kompatibel mit DRMSystem `id`“ zurück.

  `ContentKey@commonEncryptionScheme`Der Wert kann vom Schlüsselanbieter nicht überschrieben werden.
- Beim Empfang verschiedener Werte für ein `DRMSystem.ContentProtectionData <pssh>` InnerXML-Element im CPIX-Antworttext stoppt der Verschlüsseler `DRMSystem@PSSH` und gibt einen Fehler aus.

API für CPIX

- Der Schlüsselanbieter muss einen Wert für den `X-Speke-User-Agent` HTTP-Antwort-Header angeben.
- Ein SPEKE-kompatibler Verschlüsseler fungiert als Client und sendet POST-Operationen an den Endpunkt des Schlüsselanbieters.
- Der Verschlüsseler muss einen Wert für den `X-Speke-Version` HTTP-Anforderungsheader enthalten, wobei die SPEKE-Version, die bei der Anfrage verwendet wurde, formuliert ist als. MajorVersion MinorVersion, wie '2.0' für SPEKE v2.0. Wenn der Schlüsselanbieter die vom Verschlüsseler für die aktuelle Anfrage verwendete SPEKE-Version nicht unterstützt, gibt der Schlüsselanbieter einen Fehler mit der Beschreibung „SPEKE-Version nicht unterstützt“ zurück und versucht nicht, das CPIX-Dokument nach bestem Wissen zu verarbeiten.

Der vom Verschlüsseler definierte `X-Speke-Version` Header-Wert kann vom Schlüsselanbieter in der Antwort auf die Anfrage nicht geändert werden.

- Beim Empfang von Fehlern im Antworttext gibt der Verschlüsseler einen Fehler aus und versucht die Anfrage nicht erneut mit einer SPEKE v1.0-Version.

  Wenn der Schlüsselanbieter keinen Fehler zurückgibt, aber kein CPIX-Dokument zurückgibt, das die obligatorischen Informationen enthält, sollte der Verschlüsseler den Vorgang beenden und einen Fehler ausgeben.

In der folgenden Tabelle sind die Standardnachrichten zusammengefasst, die vom Schlüsselanbieter im Hauptteil der Nachricht zurückgegeben werden müssen. In Fehlerfällen muss der HTTP-Antwortcode 4XX oder 5XX sein, niemals 200. Der 422-Fehlercode kann für alle Fehler im Zusammenhang mit SPEKE/CPIX verwendet werden.

Fehlerfall	Fehlermeldung
CPIX @contentId ist nicht definiert	CPIX @contentId fehlt
CPIX @version ist nicht definiert	CPIX @version fehlt
CPIX @version wird nicht unterstützt	CPIX @version wird nicht unterstützt
ContentKey@ commonEncryptionScheme ist nicht definiert	ContentKey@ commonEncryptionScheme für KID fehlt `id` (wo dem Wert ContentKey @kid `id` entspricht)
In einem einzigen CPIX-Dokument werden mehrere ContentKey commonEncryptionScheme @-Werte verwendet	Nicht konforme @-Kombination ContentKey commonEncryptionScheme
ContentKey@ commonEncryptionScheme ist nicht mit der DRM-Technologie kompatibel	ContentKey@ ist commonEncryptionScheme nicht kompatibel mit DRMSystem `id` (wo dem `id` Wert DRMSystem @systemId entspricht)
X-Speke-Version Der Header-Wert ist keine unterstützte SPEKE-Version	SPEKE-Version wird nicht unterstützt

Fehlerfall	Fehlermeldung
Der Verschlüsselungsvertrag ist falsch formatiert	Fehlerhafter Verschlüsselungsvertrag
Der Verschlüsselungsvertrag widerspricht den Einschränkungen der DRM-Sicherheitsstufen	Der angeforderte CPIX-Verschlüsselungsvertrag wird nicht unterstützt
Der Verschlüsselungsvertrag enthält keine OR-Elemente VideoFilter AudioFilter	Fehlender CPIX-Verschlüsselungsvertrag

SPEKE API v2 — Standard-Payload-Komponenten

Durch eine einzige SPEKE-Anfrage kann der Verschlüsseler mehrere Inhaltsschlüssel zusammen mit der erforderlichen Manifestsignalisierung für mehrere Verpackungsformate anfordern, je nach dem Verschlüsselungsvertrag, der für einen bestimmten Inhalt definiert ist.

Um all diese Aspekte abzudecken, besteht ein Standard-CPIX-Dokument aus drei obligatorischen Listenabschnitten sowie einem optionalen Listenabschnitt für die Schlüsselrotation bei Live-Inhalten.

<cpix:CPIX><cpix: ContentKeyList > Abschnitt und Element der obersten Ebene

Dies ist ein obligatorischer Abschnitt, der sowohl für Live- als auch für VOD-Streaming relevant ist und die verschiedenen Inhaltsschlüssel definiert, die vom Verschlüsseler verwendet werden müssen. Das `<cpix:ContentKeyList>` Element kann ein oder mehrere `<cpix:ContentKey>` untergeordnete Elemente enthalten, von denen jedes einen eigenen Inhaltsschlüssel beschreibt.

Gemäß der CPIX-Spezifikation sind die möglichen Werte des `ContentKey@commonEncryptionScheme` Attributs in der Spezifikation Common Encryption in ISO-Basisdateien für Mediendateien (ISO/IEC 23001-7:2016) definiert:

- 'cenc': Verschlüsselung von Vollproben im AES-CTR-Modus und Video-NAL-Untermusterverschlüsselung
- 'cbc1': AES-CBC-Modus für vollständige Stichproben und Video-NAL-Teilmusterverschlüsselung
- 'cens': Partielle Video-NAL-Musterverschlüsselung im AES-CTR-Modus
- 'cbcs': Partielle Video-NAL-Musterverschlüsselung im AES-CBC-Modus

Das folgende Beispiel zeigt ein CPIX-Dokument mit einem einzigen, unverschlüsselten Inhaltsschlüssel:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 ...
</cpix:CPIX>
```

Standardmäßig sind Inhaltsschlüssel nicht verschlüsselt, wie im Beispiel unten. Die Verschlüsselung von Inhaltsschlüsseln kann jedoch vom Verschlüsseler mithilfe des Elements <cpix : >angefordert werden. DeliveryDataList Weitere Informationen finden Sie im Abschnitt Verschlüsselung von Inhaltsschlüsseln.

Element, das von SPEKE unterstützt wird	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix:CPIX>	Inhalts-ID, Version, xmlns: cpix, xmlns: pskc	name, xmlns:enc	eins <cpix: ContentKe yList >, eins<cpix : List>, eins <cpix : >DRMSyste mContentK eyUsageRuleList	ein <cpix: DeliveryDataList ContentKe yPeriodList >, eins <cpix : >
<cpixCont entKeyList: >	-	id	mindesten s ein <cpix : >ContentKey	-

Element, das von SPEKE unterstützt wird	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : >ContentKey	Kind, Data commonEncryptionScheme	id, Algorithmus, explizite IV	eins <pskc:Secret>	-
<pskc:Secret>	PlainValue oder EncryptedValue	Wert MAC	-	<enc: EncryptionMethod >, <enc : >CipherData

<cpix : Liste>Abschnitt DRMSystem

Dies ist ein obligatorischer Abschnitt, der sowohl für Live- als auch für VOD-Streaming relevant ist und in dem die verschiedenen DRM-Systeme definiert werden, die zusammen mit den Inhaltsschlüsseln genutzt werden müssen.

Das folgende Beispiel zeigt eine DRM-Systemliste mit einer einzigen PlayReady DRM-Systemspezifikation:

```
<cpix:DRMSystemList>
 <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">HicXmbZ2m[...]jEi</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
  <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
 </cpix:DRMSystem>
</cpix:DRMSystemList>
```

Eine vollständige Liste der DRM-Systeme IDs finden Sie im Abschnitt Content Protection des DASH-IF Identifiers-Repositorys.

Element, das von SPEKE unterstützt wird	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : Liste>DRM System	-	id	mindesten s ein <cpix : >DRMSystem	-
<cpix : >DRMSystem	Kind, SystemID	ID, Name, PSSH	-	ContentPr otectionData, SmoothStr eamingPro tectionHe aderData, zwei <cpix: HLSSignaling Data>-Elemente mit unterschi edlichen Playlist-Attributwerten

`DRMSystem@PSSH`ist obligatorisch, wenn die ISO-BMFF-Kapselung auf Mediensegmente angewendet wird. `DRMSystem.ContentProtectionData`Das `<pssh>` InnerXML-Element wird vom Verschlüsseler nur für manifeste Signalzwecke genutzt.

Wenn vorhanden `DRMSystem@PSSH` ist und ein `<pssh>` InnerXML-Element `DRMSystem.ContentProtectionData` enthält, müssen beide Werte identisch sein.

Wenn die `DRMSystem` Signalisierung in HLS-Manifesten erfolgen soll, müssen sowohl a `<cpix:HLSSignalingData playlist="media">` - als auch `<cpix:HLSSignalingData playlist="master">` a-Elemente in der CPIX-Anfrage und -Antwort enthalten sein.

<cpix : >Abschnitt ContentKeyPeriodList

Dies ist ein optionaler Abschnitt, der nur für Live-Streaming relevant ist und in dem die Krypto-Perioden definiert werden, die auf den Inhalt angewendet werden.

Das `<cpix:ContentKeyPeriodList>` Element kann ein oder mehrere `<cpix:ContentKeyPeriod>` untergeordnete Elemente enthalten, von denen jedes eine bestimmte Krypto-Periode in der Live-Timeline beschreibt. Die Verwendung UUIDs als Teil des Werts des ID-Attributs ist ein häufig verwendeter Ansatz.

```
<cpix:ContentKeyPeriodList>
 <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" index="1" /
>
</cpix:ContentKeyPeriodList>
```

Element, das von SPEKE unterstützt wird	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : >ContentK eyPeriodList	-	id	mindesten s ein <cpix : >ContentK eyPeriod	-
<cpix : >ContentK eyPeriod	ID, Index	-	-	-

Wenn Kryptoperioden verwendet werden, müssen die Verschlüsselungsschlüssel auch an eine der Kryptoperioden im CPIX-Dokument angehängt werden, wie im folgenden Abschnitt gezeigt.

<cpix : >Abschnitt ContentKeyUsageRuleList

Dies ist ein obligatorischer Abschnitt, der sowohl für Live- als auch für VOD-Streaming relevant ist und definiert, wie die verschiedenen Inhaltsschlüssel Tracks innerhalb des Streamsets und während der Krypto-Perioden schützen.

Das <cpix: ContentKeyUsageRuleList > -Element kann ein oder mehrere untergeordnete <cpix: ContentKeyUsageRule > -Elemente enthalten, von denen jedes die Spuren beschreibt, auf die der Verschlüsseler einen bestimmten Inhaltsschlüssel angewendet hat, möglicherweise während einer bestimmten Kryptoperiode. In einem <cpix: AudioFilter > -Element muss mindestens ein <cpix : >- oder ein <cpix: VideoFilter > -Element vorhanden sein. ContentKeyUsageRule

Das folgende Beispiel zeigt eine einfache Liste mit nur einer Regel, die einen einzigen Inhaltsschlüssel auf alle Audio- und Videotracks während einer bestimmten Kryptoperiode anwendet.

```
<cpix:ContentKeyUsageRuleList>
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="ALL">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Element, das von SPEKE unterstützt wird	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : >ContentKeyUsageRuleList	-	id	mindestens ein <cpix : >ContentKeyUsageRule	-
<cpix : >ContentKeyUsageRule	Kind, intendedTrackType	-	mindestens ein <cpix: AudioFilter > oder ein <cpix : >(*) VideoFilter	<cpix : >KeyPeriodFilter
<cpix : >KeyPeriodFilter	Perioden-ID	-	-	-
<cpix : >AudioFilter	-	Min. Kanäle, Max. Kanäle	-	-
<cpix : >VideoFilter	-	MinPixels, MaxPixels, hdr, MinFPS, MaxFPS	-	-

(*) Eine ausführliche Erklärung zur Verwendung einzelner oder mehrerer Inhaltsschlüssel zum Schutz eines oder mehrerer Tracks in einem Streamset finden Sie in der Dokumentation zum Verschlüsselungsvertrag. _

SPEKE API v2 - Verschlüsselungsvertrag

Der Verschlüsselungsvertrag legt auf der Grundlage der Eigenschaften der Tracks fest, welche Inhaltsschlüssel welche Tracks innerhalb eines bestimmten Streamsets schützen.

Die Verwendung mehrerer Inhaltsschlüssel für verschiedene Titel in einem Streamset ist zwar eine in der Branche empfohlene bewährte Methode, ist aber nicht verpflichtend, wird aber empfohlen — mindestens zwei verschiedene Inhaltsschlüssel, einer für Audiotracks und einer für Videotracks. Die Verwendung eines einzigen Inhaltsschlüssels zur Verschlüsselung mehrerer Titel ist möglich, muss aber in dem vom Verschlüsseler an den Schlüsselanbieter gesendeten CPIX-Dokument explizit angegeben werden. Im Allgemeinen beschreibt der Verschlüsseler immer genau, wie viele Inhaltsschlüssel benötigt werden und wie sie zur Verschlüsselung der verschiedenen Medientracks genutzt werden.

Prinzipien

Der Verschlüsselungsvertrag befindet sich im `<cpix:ContentKeyUsageRuleList>` Abschnitt des CPIX-Dokuments. In diesem Abschnitt entspricht jeder in diesem `<cpix:ContentKeyList>` Abschnitt definierte Inhaltsschlüssel einem bestimmten `<cpix:ContentKeyUsageRule>` Element, das Folgendes beinhalten muss:

- ein `ContentKeyUsageRule@intendedTrackType` Attribut, das auf eine oder mehrere Unterkomponenten verweisen kann, getrennt durch das Zeichen „+“, wenn mehrere Unterkomponenten verwendet werden. Der Wert von `ContentKeyUsageRule@intendedTrackType` muss in einem Verschlüsselungsvertrag einmalig sein und kann nicht in mehreren `ContentKeyUsageRule` Elementen verwendet werden.
- ein oder mehrere `<cpix:AudioFilter>` oder `<cpix:VideoFilter>` untergeordnete Elemente, abhängig vom Wert des `ContentKeyUsageRule@intendedTrackType` Attributs.

Für diese Beziehung gelten die folgenden Regeln:

- Wenn alle Audio- und Videotracks des Streamsets mit einem eindeutigen Inhaltsschlüssel geschützt werden müssen, `'ALL'` muss die Zeichenfolge als `ContentKeyUsageRule@intendedTrackType` Attributwert verwendet werden. Beispiel 1 zeigt einen solchen Anwendungsfall. In dieser Situation müssen `<cpix:AudioFilter />` sowohl

ein als auch ein `<cpix:VideoFilter />` untergeordnetes Element ohne Attribut enthalten sein. Jede andere Kombination von `<cpix:AudioFilter>` und/oder `<cpix:VideoFilter>` Elementen ist in diesem speziellen Kontext ungültig.

- Für alle anderen Anwendungsfälle kann der Wert des `ContentKeyUsageRule@intendedTrackType` Attributs frei definiert werden, und die Anzahl der `<cpix:AudioFilter />` `<cpix:VideoFilter />` untergeordneten Elemente muss der Anzahl der Unterkomponenten entsprechen, die durch das Pluszeichen aggregiert werden. Die Beispiele 2/3/4/5/6/7/9/10 veranschaulichen diese Anforderung, wenn eine einzelne Unterkomponente im Attributwert vorhanden ist. `ContentKeyUsageRule@intendedTrackType` Beispiel 8 verdeutlicht die Verwendung mehrerer Unterkomponenten: `ContentKeyUsageRule@intendedTrackType="SD+HD"` wird durch zwei unterschiedliche `<cpix:VideoFilter>` untergeordnete Elemente mit unterschiedlichen Attributwerten beschrieben und `ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"` wird durch drei unterschiedliche untergeordnete Elemente mit unterschiedlichen Attributwerten beschrieben. `<cpix:VideoFilter>`

Filter

CPIX definiert mehrere Filterelemente und Attribute, aber SPEKE unterstützt nur eine Teilmenge davon. Die folgende Tabelle fasst diese Unterschiede zusammen:

CPIX-Filtertyp	Allgemeine SPEKE-Unterstützung	Von SPEKE unterstützte Filterattribute	Filterattribute werden von SPEKE nicht unterstützt
<cpix : >VideoFilter	Ja	minPixels, maxPixels, hdr, minFps, maxFPS (optionale Attribute)	wcg
<cpix : >AudioFilter	Ja	minChannels, maxChannels (optionale Attribute)	
<cpix : >KeyPeriodFilter	Ja	PeriodID (obligatorisches Attribut)	
<cpix : >BitrateFilter	Nein	N/A	N/A

CPIX-Filtertyp	Allgemeine SPEKE-Unterstützung	Von SPEKE unterstützte Filterattribute	Filterattribute werden von SPEKE nicht unterstützt
<cpix : >LabelFilter	Nein	N/A	N/A

Gemäß der CPIX-Spezifikation für ist [minPixels VideoFilter, maxPixels] ein All-Inclusive-Bereich in beiden Dimensionen, während (minFPS, maxFPS] nur für die maxFPS-Dimension inklusiv ist. Denn [minChannels AudioFilter, maxChannels] ist ein inklusiver Bereich in beiden Dimensionen.

Problematische Situationen

Es gibt Situationen, in denen die im Verschlüsselungsvertrag enthaltenen Informationen unvollständig, mehrdeutig oder falsch sein können. In diesen Fällen ist es wichtig, dass sich der Verschlüsseler und der Schlüsselanbieter angemessen verhalten und einen angemessenen Schutz der Inhalte gewährleisten. Die folgende Tabelle zeigt das empfohlene Verhalten in diesen Situationen:

In dieser Situation	Der Verschlüsseler sollte/soll...	Der Schlüsselanbieter sollte/soll...
Für einen oder mehrere Titel im Streamset gilt keine Regel (siehe Beispiel 3 unten)	Der Verschlüsseler sollte sich seine Konfiguration (außerhalb der CPIX-Payload) ansehen und sicherstellen, dass die betreffenden Tracks nicht verschlüsselt werden müssen. Wenn dies nicht den Erwartungen entsprich t, sollte der Verschlüsseler einen Fehler ausgeben und die Verarbeitung beenden.	Nicht relevant: Der Schlüssel anbieter hat keine Kenntnis von der Streamset-Struktur.
Mehrere Regeln überschne iden sich und schlagen mehrere Inhaltsschlüssel vor,	Der Verschlüsseler sollte den zuletzt ContentKeyUsageRul e erfolgreich bewerteten	Nicht relevant: Der Schlüssel anbieter hat keine Kenntnis von der Streamset-Struktur.

In dieser Situation	Der Verschlüsseler sollte/soll...	Der Schlüsselanbieter sollte/ soll...
um einen bestimmten Titel zu verschlüsseln	Code in der Reihenfolge des Dokuments anwenden.	
Der Verschlüsselungsvertrag ändert sich in einem einzigen SPEKE-Anforderungs-/Antwort zyklus	Der Verschlüsseler muss eine Ausnahme auslösen und die Verarbeitung beenden, da der Schlüsselanbieter nicht für die Definition des Verschlüs selungsvertrags verantwortlich ist.	Um zu verhindern, dass diese Situation von vornherein eintritt, darf der Schlüssel anbieter einen Verschlüs selungsvertrag, der in der CPIX-Payload der SPEKE-Anf rage empfangen wurde, nicht ändern.
Falsch formatierter Verschlüs selungsvertrag: Ausnahme mit intendedTrackType Kardinali tätseinschränkungen /Filters, nicht unterstützte Filter oder Attribute	Der Verschlüsseler muss eine Ausnahme auslösen, die Verarbeitung beenden und die SPEKE-Anfrage nicht an den Schlüsselanbieter senden, da dies höchstwahrscheinlich zu einem fehlerhaften Schutz der Inhalte führen oder einige Spuren ungeschützt lassen würde.	Der Schlüsselanbieter löst eine Ausnahme aus und gibt die Fehlermeldung „Fehlerha fter Verschlüsselungsvertrag“ zurück.
Gut formulierter Verschlüs selungsvertrag, der jedoch gegen die DRM-Sicherheitsreg eln verstößt: Beispielsweise wird ein einziger Inhaltssc hlüssel angefordert, um sowohl Audiotracks als auch UHD-Videotracks zu schützen	Wenn der Verschlüsseler die Einschränkungen der DRM-Sicherheitsstufen kennt, sollte er eine Ausnahme auslösen, die Verarbeitung beenden und die SPEKE-Anfrage nicht an den Schlüsselanbieter senden, da dies höchstwahrscheinli ch zum Schutz fehlerhafter Inhalte führen würde.	Der Schlüsselanbieter muss eine Ausnahme auslösen und den Fehler „Angeford erter CPIX-Verschlüsselu ngsvertrag wird nicht unterstüt zt“ zurückgeben.

In dieser Situation	Der Verschlüsseler sollte/soll...	Der Schlüsselanbieter sollte/soll...
Fehlender Verschlüsselungsvertrag	Der Verschlüsseler darf keine CPIX-Dokumente versenden, die kein OE-Element enthalten . VideoFilter AudioFilter	Der Schlüsselanbieter löst eine Ausnahme aus und gibt die Fehlermeldung „Fehlender CPIX-Verschlüsselungsvertrag“ zurück.

Beispiele für Verschlüsselungsverträge

Beispiel 1: Ein Inhaltsschlüssel für alle Audio- und Videotracks

```
<cpix:ContentKeyUsageRuleList>
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="ALL">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 2: ein Inhaltsschlüssel für alle Videospuren, ein Inhaltsschlüssel für alle Audiospuren

```
<cpix:ContentKeyUsageRuleList>
    <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
       <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
       <cpix:VideoFilter />
    </cpix:ContentKeyUsageRule>
    <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
       <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
       <cpix:AudioFilter />
    </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 3: ein Inhaltsschlüssel für alle Videospuren, unverschlüsselte Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 4: mehrere Inhaltsschlüssel für verschiedene Videospuren (SD/HD), ein Inhaltsschlüssel für alle Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD video tracks (more than 1024x576) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 5: mehrere Inhaltsschlüssel für verschiedene Videospuren (SD/HD/UHD), ein Inhaltsschlüssel für alle Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
```

```
 <!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD video tracks (more than 1920x1080) -->
 <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
 intendedTrackType="UHD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 6: mehrere Inhaltsschlüssel für verschiedene Videospuren (SD/HD/UHD1/UHD2), ein Inhaltsschlüssel für alle Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
 <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
 intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD2 video tracks (more than 4096x2160) -->
```

```
 <cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
 intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 7: mehrere Inhaltsschlüssel für verschiedene Videospuren (SD/HD1/HD2/UHD1/UHD2), ein Inhaltsschlüssel für alle Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD1 video tracks (more than 1024x576, up to 1280x720) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="921600" />
 </cpix:ContentKeyUsageRule>
        <!-- Rule for HD2 video tracks (more than 1280x720, up to 1920x1080) -->
          <cpix:ContentKeyUsageRule kid="cda406d8-9d87-4f76-92da-31110e756176"
 intendedTrackType="HD2">
            <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
            <cpix:VideoFilter minPixels="921601" maxPixels="2073600" />
          </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
 <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
 intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD2 video tracks (more than 4096x2160) -->
```

```
 <cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
 intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 8: mehrere Inhaltsschlüssel für verschiedene Videospuren (basierend auf mehreren Attributtypen), ein Inhaltsschlüssel für alle Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD and HD video tracks-->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD+HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="442368" maxFps="30" hdr="false"/>
  <cpix:VideoFilter minPixels="442369" maxPixels="2073600" maxFps="30" hdr="false"/>
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HDR, HFR and UHD video tracks-->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HDR+HFR+UHD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter hdr="true" />
  <cpix:VideoFilter minFps="30" />
  <cpix:VideoFilter minPixels="20736001" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks-->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 9: eine Inhaltstaste für alle Videospuren, mehrere Inhaltstasten für Stereo- und Mehrkanal-Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for video tracks-->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for stereo audio tracks-->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
 </cpix:ContentKeyUsageRule>
 <!-- Rule for multichannel audio tracks-->
 <cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
 intendedTrackType="MULTICHANNEL_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <AudioFilter minChannels="3"/>
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Beispiel 10: ein Inhaltstasten für alle Videospuren, mehrere Inhaltstasten für Stereo und zwei Arten von Mehrkanal-Audiospuren

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for video tracks-->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for stereo audio tracks-->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
 </cpix:ContentKeyUsageRule>
 <!-- Rule for multichannel audio tracks (3 to 6 channels)-->
 <cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
 intendedTrackType="MULTICHANNEL_AUDIO_3_6">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="3" maxChannels="6"/>
 </cpix:ContentKeyUsageRule>
```

```
  <!-- Rule for multichannel audio tracks (7 channels and more)-->
 <cpix:ContentKeyUsageRule kid="81eb3761-55ff-4d22-a31d-94f01bbfd8ba"
 intendedTrackType="MULTICHANNEL_AUDIO_7">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="7"/>
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

SPEKE API v2 — Beispiele für Live-Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Die folgende URL ist lediglich ein Beispiel und gibt kein bestimmtes Format vor:

```
POST https://speke-compatible-server/speke/v2.0/copyProtection
```

Anforderungstext

Ein CPIX-Dokument.

Anforderungs-Header

Name	Typ	Auftreten	Beschreibung
`AWS Authorization`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`X-Amz-Security-Token`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`X-Amz-Date`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	SPEKE-API-Version, die mit der Anfrage verwendet wurde,

Name	Typ	Auftreten	Beschreibung
			formuliert als. MajorVersion MinorVersion, wie '2.0' für SPEKE v2.0

Antwort-Header

Name	Typ	Auftreten	Beschreibung
`X-Speke-User-Agent`	String	1..1	Zeichenfolge, die den Schlüsselanbieter identifiziert.
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	SPEKE-API-Version, die mit der Anfrage verwendet wurde, formuliert als. MajorVersion MinorVersion, wie '2.0' für SPEKE v2.0

Request Response (Antwort anfordern)

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`200 (Success)`	CPIX	1..1	DASH-CPIX-Nutzlastantwort
`4XX (Client error)`	Client-Fehlermeldung	1..1	Beschreibung des Client-Fehlers.
`5XX (Server error)`	Server-Fehlermeldung	1..1	Beschreibung des Server-Fehlers.

> **Note**
>
> Die Beispiele in diesem Abschnitt zeigen keine Inhaltsschlüssel-Verschlüsselung. Informationen zum Hinzufügen von Inhaltsschlüsselverschlüsselung finden Sie unter Inhaltsschlüsselverschlüsselung.

Beispiel für eine Live-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Payload für Live-Anfragen vom Verschlüsseler an den DRM-Schlüsselanbieter mit einem Inhaltsschlüssel für alle Videospuren und einem Inhaltsschlüssel für alle Audiospuren:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
```

```
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
```

```
</cpix:CPIX>
```

Beispiel für eine Live-Antwortnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Antwortnutzlast des DRM-Schlüsselanbieters (die zurückgegebenen Werte wurden aus Gründen der Lesbarkeit mit [...] gekürzt):

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>h3toSFIlyAYpfXVQ795m6x==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
```

```
    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
   </cpix:DRMSystem>
   <!-- Playready -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
   <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
  index="1" />
  </cpix:ContentKeyPeriodList>
  <cpix:ContentKeyUsageRuleList>
   <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
   </cpix:ContentKeyUsageRule>
   <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
```

```
    <cpix:AudioFilter />
   </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2 — Beispiele für VOD-Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Die folgende URL ist lediglich ein Beispiel und gibt kein bestimmtes Format vor.

```
POST https://speke-compatible-server/speke/v2.0/copyProtection
```

Anforderungstext

Ein CPIX-Dokument.

Anforderungs-Header

Name	Typ	Auftreten	Beschreibung
`AWS Authorization`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`X-Amz-Security-Token`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`X-Amz-Date`	String	1..1	Weitere Informationen finden Sie unter AWS Sigv4.
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	SPEKE-API-Version, die mit der Anfrage verwendet wurde, formuliert als.

Name	Typ	Auftreten	Beschreibung
			MajorVersion MinorVersion, wie '2.0' für SPEKE v2.0

Antwort-Header

Name	Typ	Auftreten	Beschreibung
`X-Speke-User-Agent`	String	1..1	Zeichenfolge, die den Schlüsselanbieter identifiziert.
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	SPEKE-API-Version, die mit der Anfrage verwendet wurde, formuliert als. MajorVersion MinorVersion, wie '2.0' für SPEKE v2.0

Request Response (Antwort anfordern)

HTTP-CODE	Name der Nutzlast	Auftreten	Beschreibung
`200 (Success)`	CPIX	1..1	DASH-CPIX-Nutzlast antwort
`4XX (Client error)`	Client-Fehlermeldung	1..1	Beschreibung des Client-Fehlers.
`5XX (Server error)`	Server-Fehlermeldung	1..1	Beschreibung des Server-Fehlers.

> **Note**
>
> Die Beispiele in diesem Abschnitt zeigen keine Inhaltsschlüssel-Verschlüsselung. Informationen zum Hinzufügen von Inhaltsschlüsselverschlüsselung finden Sie unter Inhaltsschlüsselverschlüsselung.

Beispiel für eine VOD-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Payload für VOD-Anfragen vom Verschlüsseler an den DRM-Schlüsselanbieter mit einem Inhaltsschlüssel für alle Videospuren und einem Inhaltsschlüssel für alle Audiospuren:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
```

```
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Beispiel für eine VOD-Antwortnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Antwort-Payload des DRM-Schlüsselanbieters (die zurückgegebenen Werte wurden aus Gründen der Lesbarkeit mit [...] gekürzt):

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>h3toSFIlyAYpfXVQ795m6x==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
   <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
```

```
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
   </cpix:DRMSystem>
   <!-- Playready -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyUsageRuleList>
   <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="VIDEO">
    <cpix:VideoFilter />
   </cpix:ContentKeyUsageRule>
   <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  intendedTrackType="AUDIO">
    <cpix:AudioFilter />
   </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2 — Verschlüsselung von Inhaltsschlüsseln

Sie können Ihrer SPEKE-Implementierung optional eine Inhaltsschlüsselverschlüsselung hinzufügen. Die Inhaltsschlüsselverschlüsselung garantiert vollständigen end-to-end Schutz, indem sie zusätzlich zur Verschlüsselung des Inhalts selbst auch die Inhaltsschlüssel für die Übertragung verschlüsselt. Wenn Sie dies nicht für Ihren Schlüsselanbieter implementieren, verlassen Sie

sich aus Sicherheitsgründen auf die Verschlüsselung der Transportschicht sowie auf eine starke Authentifizierung.

Um die Inhaltsschlüsselverschlüsselung für Verschlüsseler zu verwenden, die in der AWS-Cloud ausgeführt werden, importieren Kunden Zertifikate in den AWS Certificate Manager und verwenden das resultierende Zertifikat dann ARNs für ihre Verschlüsselungsaktivitäten. Der Verschlüsseler verwendet das Zertifikat ARNs und den ACM-Service, um verschlüsselte Inhaltsschlüssel für den DRM-Schlüsselanbieter bereitzustellen.

Einschränkungen

SPEKE unterstützt die Verschlüsselung von Inhaltsschlüsseln gemäß der DASH-IF CPIX-Spezifikation mit den folgenden Einschränkungen:

- SPEKE unterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
- SPEKE benötigt 2048 RSA-basierte Zertifikate.

Diese Einschränkungen sind auch unter Anpassungen und Einschränkungen der DASH-IF-Spezifikation aufgeführt.

Implementieren der Inhaltsschlüssel-Verschlüsselung

Um Inhaltsschlüssel-Verschlüsselung bereitzustellen, führen Sie in den Implementierungen Ihres DRM-Schlüsselanbieters Folgendes aus:

- Verarbeiten Sie das Element `<cpix:DeliveryDataList>` in den Anforderungs- und Antwortnutzlasten.
- Stellen Sie in der `<cpix:ContentKeyList>` der Antwortnutzlasten verschlüsselte Werte bereit.

Weitere Informationen zu diesen Elementen finden Sie in der DASH-IF CPIX 2.3-Spezifikation.

Beispiel für das Inhaltsschlüssel-Verschlüsselungselement `<cpix:DeliveryDataList>` in der Anforderungsnutzlast

```
<cpix:CPIX contentId="abc123"
    version="2.3"
    xmlns:cpix="urn:dashif:org:cpix"
    xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
```

```
    <cpix:DeliveryDataList>
        <cpix:DeliveryData id="<ORIGIN SERVER ID>">
            <cpix:DeliveryKey>
                <ds:X509Data>
                    <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
                </ds:X509Data>
            </cpix:DeliveryKey>
        </cpix:DeliveryData>
    </cpix:DeliveryDataList>
    <cpix:ContentKeyList>
     ...
    </cpix:ContentKeyList>
</cpix:CPIX>
```

Beispiel für das Inhaltsschlüssel-Verschlüsselungselement `<cpix:DeliveryDataList>` in der Antwortnutzlast

```
<cpix:CPIX contentId="abc123"
    version="2.3"
    xmlns:cpix="urn:dashif:org:cpix"
    xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
    <cpix:DeliveryDataList>
        <cpix:DeliveryData id="<ORIGIN SERVER ID>">
            <cpix:DeliveryKey>
                <ds:X509Data>
                    <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
                </ds:X509Data>
            </cpix:DeliveryKey>
            <cpix:DocumentKey Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc">
                <cpix:Data>
                    <pskc:Secret>
                        <pskc:EncryptedValue>
                            <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                            <enc:CipherData>
                                <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                            </enc:CipherData>
                        </pskc:EncryptedValue>
                        <pskc:ValueMAC>qnei/5TsfUwDu+8bhsZrLjDRDngvmnUZD2eva7SfXWw=</
pskc:ValueMAC>
                    </pskc:Secret>
```

```
                </cpix:Data>
            </cpix:DocumentKey>
            <cpix:MACMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-
sha512">
                <cpix:Key>
                    <pskc:EncryptedValue>
                        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                        <enc:CipherData>
                            <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                        </enc:CipherData>
                    </pskc:EncryptedValue>
                    <pskc:ValueMAC>DGqdpHUfFKxdsO9+EWrPjtdTCVfjPLwwtzEcFC/j0xY=</
pskc:ValueMAC>
                </cpix:Key>
            </cpix:MACMethod>
        </cpix:DeliveryData>
    </cpix:DeliveryDataList>
    <cpix:ContentKeyList>
     ...
    </cpix:ContentKeyList>
</cpix:CPIX>
```

Beispiel für das Inhaltsschlüssel-Verschlüsselungselement `<cpix:ContentKeyList>` in der Antwortnutzlast

Das folgende Beispiel zeigt die Behandlung des verschlüsselten Inhaltsschlüssels im `<cpix:ContentKeyList>`-Element der Antwortnutzlast. Hier wird das Element `<pskc:EncryptedValue>` verwendet:

```
<cpix:ContentKeyList>
     <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-
a20d-163a-e382420c6eff" commonEncryptionScheme="cbcs">
         <cpix:Data>
             <pskc:Secret>
                 <pskc:EncryptedValue>
                     <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
                     <enc:CipherData>
                         <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
                     </enc:CipherData>
                 </pskc:EncryptedValue>
```

```
                <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
             </pskc:Secret>
         </cpix:Data>
     </cpix:ContentKey>
 </cpix:ContentKeyList>
```

Im Vergleich dazu zeigt das folgende Beispiel eine ähnliche Antwortnutzlast mit dem unverschlüsselten Inhaltsschlüssel als entschlüsselter Schlüssel. Hier wird das Element `<pskc:PlainValue>` verwendet:

```
<cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-
a20d-163a-e382420c6eff" commonEncryptionScheme="cbcs">
        <cpix:Data>
            <pskc:Secret>
                <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
            </pskc:Secret>
        </cpix:Data>
    </cpix:ContentKey>
</cpix:ContentKeyList>
```

SPEKE API v2 — Überschreiben der Schlüssel-ID

Der Verschlüsseler erstellt bei jeder Rotation der Schlüssel eine neue Schlüssel-ID (Key Identifier, KID). Er übergibt die KID an den DRM-Schlüsselanbieter bei dessen Anforderungen. Beinahe immer antwortet der Schlüsselanbieter mit derselben KID. Er kann jedoch in der Antwort auch einen anderen Wert für die KID bereitstellen.

Im Folgenden finden Sie eine Beispielanforderung mit der KID `11111111-1111-1111-1111-111111111111`:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
 kid="11111111-1111-1111-1111-111111111111" commonEncryptionScheme="cbcs"></
cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- Widevine -->
```

```
  <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Die folgende Antwort überschreibt die KID zu `22222222-2222-2222-2222-222222222222`:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
 kid="22222222-2222-2222-2222-222222222222" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- Widevine -->
  <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
   <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
```

```
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Lizenz für die SPEKE API-Spezifikation

Creative Commons Namensnennung — ShareAlike 4.0 Internationale öffentliche Lizenz

Durch die Ausübung der lizenzierten Rechte (unten definiert) akzeptieren Sie die Bedingungen dieser Creative Commons Attribution- ShareAlike 4.0 International Public License („Öffentliche Lizenz“) und erklären sich damit einverstanden, an diese gebunden zu sein. In dem Umfang, in dem diese öffentliche Lizenz als Vertrag interpretiert werden kann, werden Ihnen die lizenzierten Rechte unter der Voraussetzung gewährt, dass Sie diesen Bestimmungen zustimmen. Der Lizenzgeber gewährt Ihnen diese Rechte aufgrund des Nutzens, der sich für den Lizenzgeber aus der Verfügbarmachung des lizenzierten Materials unter diesen Bestimmungen ergibt.

Abschnitt 1: Definitionen.

a. Adaptiertes Material bezeichnet Material, das dem Urheberrecht und vergleichbaren Schutzrechten unterliegt, das aus dem lizenzierten Material abgeleitet ist oder darauf basiert und in dem das lizenzierte Material übersetzt, geändert, angeordnet, transformiert oder anderweitig auf eine Weise modifiziert wurde, die nach Urheberrecht oder vergleichbaren Schutzrechten, die vom Lizenzgeber gehalten werden, eine Erlaubnis erforderlich machen. Im Rahmen dieser öffentlichen Lizenz, bei der das lizenzierte Material ein musikalisches Werk, eine Aufführung oder eine Audioaufnahme ist, entsteht immer adaptiertes Material, wenn das lizenzierte Material zeitlich mit bewegten Bildern synchronisiert wird.

b. Die Lizenz von Adapter bedeutet die Lizenz, die Sie gemäß den Bedingungen dieser Public License auf Ihr Urheberrecht und ähnliche Rechte an Ihren Beiträgen zu adaptiertem Material anwenden.

c. BY-SA-kompatible Lizenz bedeutet eine auf creativecommons.org/compatiblelicenses aufgeführte Lizenz, die von Creative Commons als im Wesentlichen dieser Public License gleichwertig genehmigt wurde.

d. Urheberrecht und vergleichbare Schutzrechte bezeichnen Urheberrechte und/oder vergleichbare Rechte, die eng mit dem Urheberrecht verbunden sind. Dies gilt einschließlich, ohne darauf beschränkt zu sein, Aufführungen, Sendungen, Audioaufnahmen sowie Datenbankherstellerrechte, unabhängig davon, wie die Rechte gekennzeichnet oder kategorisiert sind. Im Rahmen dieser öffentlichen Lizenz gelten die in Abschnitt 2(b) (1) – (2) nicht als Urheberrechte und vergleichbare Schutzrechte.

e. "Effektive technologische Maßnahmen" bezeichnet Maßnahmen, die bei Fehlen einer zuständigen Behörde unter Gesetzen, die die Verpflichtungen aus Artikel 11 des WIPO-Urheberrechtsvertrags in der Fassung vom 20. Dezember 1996 und/oder ähnlicher internationaler Verträge erfüllen, nicht umgangen werden dürfen.

f. Ausnahmen und Einschränkungen bezeichnen Fair Use, Fair Dealing und/oder andere Ausnahmen oder Einschränkungen in Bezug auf das Urheberrecht und vergleichbare Schutzrechte, die für Ihre Nutzung des lizenzierten Materials relevant sind.

g. Lizenzelemente sind die Lizenzattribute, die im Namen einer Creative Commons Public License aufgeführt sind. Die Lizenzelemente dieser Public License sind Namensnennung und ShareAlike.

h. Lizenziertes Material bezeichnet das künstlerische oder literarische Werk, die Datenbank oder das andere Material, das oder die der Lizenzgeber unter dieser öffentlichen Lizenz bereitstellt.

i. "Lizenzierte Rechte" bezeichnet die Rechte, die Ihnen unter den Bestimmungen dieser öffentlichen Lizenz gewährt werden und die auf alle Urheberrechte und vergleichbare Schutzrechte beschränkt sind, die für Ihre Nutzung des lizenzierten Materials, zu dessen Lizenzierung der Lizenzgeber berechtigt ist, gelten.

j. "Lizenzgeber" bezeichnet natürliche oder juristische Personen, die Rechte unter dieser öffentlichen Lizenz gewähren.

k. "Teilen" bezeichnet das Bereitstellen von Material für die Öffentlichkeit, für das eine Erlaubnis nach Maßgabe der lizenzierten Rechte erforderlich ist, mit beliebigen Mitteln oder Prozessen, also z. B. Reproduktion, öffentliche Darstellung, öffentliche Aufführung, Weitergabe, Verbreitung, Übermittlung oder Import, und das Verfügbarmachen von Material für die Öffentlichkeit unter Einschluss von Methoden, die der Öffentlichkeit den Zugriff auf das Material an selbst gewählten Orten und zu selbst gewählten Zeiten ermöglichen.

l. Datenbankherstellerrechte bezeichnen über den aus der Richtlinie 96/9/EG des europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken in der jeweils gültigen Form sowie über äquivalente Rechte weltweit hinausreichende Rechte.

m. "Sie" bezeichnet natürliche oder juristische Personen, die Rechte unter dieser öffentlichen Lizenz ausüben. Die zugehörigen Personal- und Possessivpronomen haben entsprechende Bedeutung.

Abschnitt 2: Geltungsbereich.

a. Lizenzgewährung.

1. Nach Maßgabe der Bestimmungen dieser öffentlichen Lizenz gewährt der Lizenzgeber Ihnen hiermit eine weltweite, lizenzgebührenfreie, nicht unterlizenzierbare, nicht exklusive und unwiderrufliche Lizenz, die lizenzierten Rechte in Bezug auf das lizenzierte Material auszuüben:

   A. das lizenzierte Material ganz oder teilweise zu reproduzieren und zu teilen; und

   B. adaptiertes Material zu produzieren, zu reproduzieren und zu teilen.

2. Ausnahmen und Einschränkungen. Zur Klarstellung: Sofern für Ihre Nutzung Ausnahmen und Einschränkungen gelten, findet diese öffentliche Lizenz keine Anwendung und Sie müssen ihre Bestimmungen nicht erfüllen.

3. Laufzeit. Die Laufzeit dieser öffentlichen Lizenz ist in Abschnitt 6(a) angegeben.

4. Medien und Formate; technische Modifikationen zulässig. Der Lizenzgeber berechtigt Sie, die lizenzierten Rechte in Bezug auf alle Medien und Formate auszuüben, auch wenn diese derzeit noch nicht bekannt oder noch nicht geschaffen wurden, und die zu diesem Zweck erforderlichen technischen Modifikationen vorzunehmen. Der Lizenzgeber verzichtet auf jegliche Rechte oder Ansprüche und/oder stimmt zu, keine Rechte oder Ansprüche geltend zu machen, die Ihnen das Vornehmen technischer Modifikationen untersagen, die erforderlich sind, um die lizenzierten Rechte auszuüben. Dies gilt einschließlich technischer Modifikationen, die erforderlich sind, um die effektiven technologischen Maßnahmen zu umgehen. Gemäß diesem Abschnitt 2(a)(4) zulässigerweise vorgenommene Änderungen schaffen im Rahmen dieser öffentlichen Lizenz kein adaptiertes Material.

5. Nachfolgende Empfänger.

   A. Angebot des Lizenzgebers – lizenziertes Material. Jeder Empfänger des lizenzierten Materials erhält vom Lizenzgeber automatisch ein Angebot zur Ausübung der lizenzierten Rechte unter den Bestimmungen dieser öffentlichen Lizenz.

   B. Zusätzliches Angebot des Lizenzgebers — Adaptiertes Material. Jeder Empfänger von adaptiertem Material von Ihnen erhält automatisch ein Angebot des Lizenzgebers, die

lizenzierten Rechte an dem adaptierten Material gemäß den Bedingungen der von Ihnen geltenden Adapterlizenz auszuüben.

C. Keine Einschränkungen für nachfolgende Empfänger. Sie dürfen in Bezug auf das lizenzierte Material keine zusätzlichen oder abweichenden Bestimmungen anbieten oder auferlegen oder effektive technologische Maßnahmen anwenden, wenn dies die Ausübung der lizenzierten Rechte eines Empfängers des lizenzierten Materials einschränkt.

6. Keine Billigung. Keine der Aussagen in dieser öffentlichen Lizenz begründet oder darf ausgelegt werden als eine Erlaubnis, zu behaupten oder zu implizieren, dass Sie verbunden sind mit dem, gesponsert sind vom, gebilligt werden vom oder einen offiziellen Status erhalten haben vom Lizenzgeber oder Dritten, denen eine Namensnennung nach Abschnitt 3(a)(1)(A)(i) zusteht, oder dass Ihre Nutzung des lizenzierten Materials im Rahmen einer solchen Verbindung erfolgt.

b. Andere Rechte.

1. Urheberpersönlichkeitsrechte, wie das Recht auf Integrität, sind nicht im Rahmen dieser Public License lizenziert, ebenso wenig wie Werbung und Datenschutz. Wir verpflichten uns, and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or solche Rechte, die dem Lizenzgeber zustehen, nicht in dem begrenzten Umfang geltend zu machen, der erforderlich ist, um Ihnen die Ausübung der lizenzierten Rechte zu ermöglichen, aber nicht anderweitig.
2. Patent- und Markenrechte werden unter dieser öffentlichen Lizenz nicht lizenziert.
3. Der Lizenzgeber verzichtet im möglichen Umfang auf jegliches Recht, von Ihnen auf Grundlage einer freiwilligen Lizenz oder einer gesetzlichen oder Zwangslizenz, für die ein Rechtsverzicht möglich ist, für die Ausübung der lizenzierten Rechte Gebühren zu erheben, ob direkt oder über eine Gebührenerhebungsgesellschaft. Für alle anderen Fälle behält sich der Lizenzgeber das Recht zum Erheben solcher Gebühren ausdrücklich vor.

Abschnitt 3: Lizenzbedingungen.

Die Ausübung der lizenzierten Rechte durch Sie setzt ausdrücklich die Einhaltung der folgenden Bedingungen voraus.

a. Nennung.

1. Wenn Sie das lizenzierte Material weitergeben (auch in modifizierter Form), müssen Sie Folgendes angeben:

A. Folgendes behalten, wenn es vom Lizenzgeber zusammen mit dem Lizenzmaterial geliefert wird:

```
i . identification of the creator(s) of the Licensed Material and any others
 designated to receive attribution, in any reasonable manner requested by the
 Licensor (including by pseudonym if designated);
```

```
ii . a copyright notice;
```

```
iii . a notice that refers to this Public License;
```

```
iv . a notice that refers to the disclaimer of warranties;
```

```
v . a URI or hyperlink to the Licensed Material to the extent reasonably
 practicable;
```

B. geben Sie an, ob Sie das Lizenzmaterial geändert haben, und behalten Sie einen Hinweis auf frühere Änderungen bei; und

C. geben Sie an, dass das lizenzierte Material unter dieser Public License lizenziert ist, und fügen Sie den Text, die URI oder den Hyperlink zu dieser Public License hinzu.

2. Sie können die Bedingungen in Abschnitt 3(a)(1) auf beliebige sinnvolle Weise nach Maßgabe von Medium, Mittel und Kontext erfüllen, mit und in dem Sie das lizenzierte Material weitergeben. Es kann beispielsweise sinnvoll sein, die Bedingungen durch Bereitstellung eines URI oder Hyperlinks auf eine Ressource zu erfüllen, die die erforderlichen Informationen enthält.
3. Wenn der Lizenzgeber dies fordert, müssen Sie die gemäß Abschnitt 3(a)(1)(A) erforderlichen Informationen entfernen, soweit dies praktikabel ist.

b. ShareAlike. Wenn Sie von Ihnen erstelltes adaptiertes Material teilen, gelten zusätzlich zu den Bedingungen in Abschnitt 3 (a) auch die folgenden Bedingungen.

1. Bei der Adapterlizenz, die Sie beantragen, muss es sich um eine Creative Commons-Lizenz mit denselben Lizenzelementen, in dieser Version oder einer späteren Version, oder um eine BY-SA-kompatible Lizenz handeln.
2. Sie müssen den Text oder die URI oder den Hyperlink der Adapterlizenz, die Sie beantragen, angeben. Sie können diese Bedingung auf jede angemessene Weise erfüllen, die auf dem Medium, den Mitteln und dem Kontext basiert, in dem Sie adaptiertes Material teilen.
3. Sie dürfen keine zusätzlichen oder anderen Bedingungen oder Bedingungen anbieten oder ihnen auferlegen oder wirksame technologische Maßnahmen auf adaptiertes Material

anwenden, die die Ausübung der Rechte einschränken, die im Rahmen der von Ihnen angewandten Adapterlizenz gewährt wurden.

Abschnitt 4: Datenbankherstellerrechte.

Sofern die lizenzierten Rechte Datenbankherstellerrechte umfassen, die für Ihre Nutzung des lizenzierten Materials gelten, ist Folgendes zu beachten:

a. Zur Klarstellung: Abschnitt 2 (a) (1) gewährt Ihnen das Recht, den gesamten Inhalt der Datenbank oder einen wesentlichen Teil davon zu extrahieren, wiederzuverwenden, zu reproduzieren und weiterzugeben;

b. wenn Sie den gesamten oder einen wesentlichen Teil des Datenbankinhalts in eine Datenbank aufnehmen, an der Sie Sui-Generis-Datenbankrechte haben, dann ist die Datenbank, an der Sie Sui-Generis-Datenbankrechte haben (aber nicht ihre einzelnen Inhalte), adaptiertes Material, auch für die Zwecke von Abschnitt 3 (b); und

c. Sie müssen die Bedingungen in Abschnitt 3(a) erfüllen, wenn Sie den Inhalt der Datenbank ganz oder in substanziellen Teilen weitergeben. Zur Klarstellung: Dieser Abschnitt 4 ergänzt Ihre Pflichten aus dieser öffentlichen Lizenz, sofern die lizenzierten Rechte Urheberrechte und vergleichbare Schutzrechte umfassen, und ersetzt diese Pflichten nicht.

Abschnitt 5: Gewährleistungsausschluss und Haftungsbeschränkung.

a. Sofern nicht separat anderweitig vom Lizenzgeber zugesichert, bietet der Lizenzgeber das lizenzierte Material im vollständig möglichen Umfang in der vorliegenden und verfügbaren Form an und macht keinerlei Zusicherungen und übernimmt keinerlei Garantien jedweder Art in Bezug auf das lizenzierte Material, ob ausdrücklich, implizit, aus Gesetz oder anderweitig. Dies schließt, ohne darauf beschränkt zu sein, Rechtsmängelgewähr, Handelsüblichkeit, Eignung für einen bestimmten Zweck, Nichtverletzung der Rechte Dritter, Abwesenheit latenter oder anderer Defekte, Genauigkeit sowie das Vorliegen oder Nichtvorliegen von Fehlern, ob bekannt oder erkennbar oder nicht, ein. Da ein vollständiger oder teilweiser Haftungsausschluss nicht überall zulässig ist, betrifft dieser Ausschluss Sie möglicherweise nicht.

b. Im größtmöglichen Umfang wird die Haftung des Lizenzgebers Ihnen gegenüber aus beliebigem Rechtsgrund (einschließlich Fahrlässigkeit, ohne darauf beschränkt zu sein) für unmittelbare, konkrete oder mittelbare Schäden, Nebenkosten, Folgeschäden, Strafzahlungen oder Schadenersatz mit Strafcharakter oder andere Verluste, Kosten, Ausgaben oder Schäden, die sich aus dieser öffentlichen Lizenz oder der Nutzung des lizenzierten Materials

ergeben, ausgeschlossen, auch wenn der Lizenzgeber über die Möglichkeit solcher Verluste, Kosten, Ausgaben oder Schäden informiert war. Da eine vollständige oder teilweise Haftungsbeschränkung nicht überall zulässig ist, betrifft diese Beschränkung Sie möglicherweise nicht.

c. Die angegebenen Gewährleistungsausschluss und Haftungsbeschränkungen sind so zu interpretieren, dass das Ergebnis einem vollständigen Ausschluss jeglicher Haftung möglichst nahekommt.

Abschnitt 6: Laufzeit und Beendigung.

a. Die Geltungsdauer dieser öffentlichen Lizenz entspricht der Geltungsdauer der in dieser Lizenz lizenzierten Urheberrechte und vergleichbaren Schutzrechte. Falls Sie jedoch gegen Bestimmungen dieser öffentlichen Lizenz verstoßen, enden Ihre Rechte aus dieser öffentlichen Lizenz automatisch.

b. Sofern Ihr Recht zur Nutzung des lizenzierten Materials gemäß Abschnitt 6(a) beendet wurde, wird es in folgenden Situationen wiederhergestellt:

   1. automatisch ab dem Tag, an dem der Verstoß behoben ist, sofern er innerhalb von 30 Tagen nach Ihrer Entdeckung des Verstoßes behoben wird; oder
   2. nach ausdrücklicher Wiedereinstellung durch den Lizenzgeber.

c. Zur Klarstellung: Dieser Abschnitt 6(b) beeinträchtigt in keiner Weise die Rechte des Lizenzgebers, Ihnen gegenüber Rechtsmittel aufgrund Ihrer Verstöße gegen diese öffentliche Lizenz zu ergreifen.

d. Zur Klarstellung: Der Lizenzgeber darf das lizenzierte Material auch unter anderen Bestimmungen anbieten sowie jederzeit die Weitergabe des lizenzierten Materials stoppen. Dadurch wird aber diese öffentliche Lizenzen nicht beendet.

e. Die Abschnitte 1, 5, 6, 7 und 8 gelten nach Beendigung dieser öffentlichen Lizenz fort.

Abschnitt 7: Andere Bestimmungen.

a. Der Lizenzgeber wird durch zusätzliche oder abweichende Bestimmungen in Mitteilungen von Ihnen nicht gebunden, sofern dies nicht ausdrücklich vereinbart wird.

b. Alle Arrangements, Absprachen oder Verträge in Bezug auf das lizenzierte Material, die nicht in diesem Dokument enthalten sind, gelten separat und unabhängig von den Bestimmungen dieser öffentlichen Lizenz.

Abschnitt 8: Interpretation.

a. Zur Klarstellung: Diese öffentliche Lizenz stellt keine Einschränkung, Limitierung oder Beschränkung einer Nutzung des lizenzierten Materials dar, unterwirft diese Nutzung keinen Bedingungen und darf nicht interpretiert werden, als wäre dies ihr Zweck, sofern die betreffende Nutzung rechtmäßig ohne Erlaubnis durch diese öffentliche Lizenz möglich wäre.
b. In dem Umfang, in dem eine Bestimmung dieser öffentlichen Lizenz als undurchsetzbar gefunden wird, wird sie automatisch in geringstmöglichem Umfang umgeformt, um ihre Durchsetzbarkeit zu ermöglichen. Kann die Bestimmung nicht umgeformt werden, ist sie von dieser öffentlichen Lizenz abzutrennen, ohne dass dies die Durchsetzbarkeit der übrigen Bestimmungen beeinträchtigen würde.
c. Ein Rechtsverzicht auf eine der Bestimmungen dieser öffentlichen Lizenz sowie eine Zustimmung zu einem Verstoß gegen die Bestimmungen dieser öffentlichen Lizenz ist nur durch ausdrückliche Vereinbarung seitens des Lizenzgebers möglich.
d. Keine der Aussagen in dieser öffentlichen Lizenz begründet oder darf interpretiert werden als eine Beschränkung der oder ein Verzicht auf Rechte und Privilegien, die für den Lizenzgeber oder Sie gelten, einschließlich der aus rechtlichen Verfahren von Jurisdiktionen oder Behörden erwachsenden Rechte und Privilegien.

Dokumentenhistorie für den SPEKE Partner- und Kundenführer

In der folgenden Tabelle werden die Änderungen an der SPEKE-Dokumentation beschrieben.

SPEKE v1

Änderung	Beschreibung	Datum
Support-Matrix: Services und Produkte von AWS-Partnern	Es wurde ein neuer Abschnitt für SPEKE-Support in den Services und Produkten von AWS-Partnern hinzugefügt, in dem die Bitmovin-Services aufgeführt sind.	13. Januar 2023
Updates für DRM-Platt formanbieter	Es wurden Links und neue Partnerinformationen zur DRM-Plattformanbieterliste hinzugefügt.	24. Januar 2019
Drittanbieter-Verschlüsseler einschließen	Architektur und Beschreib ungen wurden aktualisiert, um Drittanbieter-Verschlüsseler zu berücksichtigen.	20. November 2018
Inhaltsschlüssel-Verschlüss elung	Hinzufügung der Option für die Verschlüsselung von Inhaltssc hlüsseln. Zuvor unterstüt zten Secure Packager und Encoder Key Exchange nur die Lieferung von Klarschlü sseln.	30. Oktober 2018
Unterstützungsmatrix — AWS Elemental Live	Hinzufügung einer AWS Elemental Live-Unterstützung smatrix.	27. September 2018

Änderung	Beschreibung	Datum
Nutzlast-Standardkomponente n	Hinzufügung eines Abschnitt s, der die Hauptelemente einer JSON-Nutzlast definiert.	27. September 2018
KID-Überschreibung	Hinzufügung eines Abschnitt s über KID Überschreibungen durch einen Schlüsselanbieter.	27. September 2018
Korrigierte Links zur DASH-IF-Website	Die Links zur DASH IF-Seite für die CPIX-Spezifikation und die Systemseite wurden korrigiert. IDs	27. September 2018
Veröffentlichung eines Texts für AWS Elemental Live.	Die SPEKE-Dokumentatio n wurde aktualisiert, um AWS Elemental-Produkte zu berücksichtigen.	20. Juli 2018
CMAF	Die Unterstützungsmatr ixtabellen für Services wurden aktualisiert, damit sie das CMAF (Common Media Application Format) enthalten.	27. Juni 2018

Änderung	Beschreibung	Datum
Erstversion	Erste Version von Secure Packager and Encoder Key Exchange (SPEKE) Version 1, einer Spezifikation für die Kommunikation zwischen einem Inhaltsverschlüsseler und einem DRM-Schlüsselanbieter. Der DRM-Schlüsselanbieter stellt eine Secure Packager- und Encoder Key Exchange-API zur Bearbeitung eingehender Schlüsselanfragen zur Verfügung.	27. November 2017

SPEKE v2

Änderung	Beschreibung	Datum
Aktualisierungen im Bereich DRM-Plattformanbieter und im Bereich AWS-Dienste und -Produkte, die SPEKE unterstützen	Webstream wurde zur SPEKE v2-Spalte der Liste der DRM-Plattformanbieter hinzugefügt und MediaConvert zur SPEKE v2-Spalte der Tabelle SPEKE-Support in AWS-Services und -Produkten hinzugefügt.	10. Oktober 2024
Aktualisierungen im Bereich DRM-Plattformanbieter	Neue qualifizierte Partner wurden zur SPEKE v2-Spalte der Liste der DRM-Plattformanbieter hinzugefügt.	9. August 2023
Aktualisierungen der Abschnitte mit Beispielen für Live- und VOD-Workflow-Methodenaufrufe	In den Abschnitten mit Beispielen für SPEKE v2 Live- und VOD-Workflow-Methodenaufrufe wurde ein	13. Januar 2023

Änderung	Beschreibung	Datum
	fehlender X-Speke-Version Antwort-Header hinzugefügt.	
Aktualisierungen im Abschnitt „Anbieter von DRM-Platt formen“ und „Verschlü sselungsverträge“	Neue qualifizierte Partner wurden zur SPEKE v2-Spalte der Liste der DRM-Plattformanbieter hinzugefü gt. Zwei neue Beispiele für Verschlüsselungsverträge wurden hinzugefügt und die maximale SD-Auflösung in allen betroffenen Beispielen auf 1024x576 geändert.	27. Januar 2022
Erstversion	Erste Version von Secure Packager and Encoder Key Exchange (SPEKE), Version 2.0, einer Spezifikation für die Kommunikation zwischen einem Inhaltsverschlüsse ler und einem DRM-Schlü sselanbieter. Der DRM-Schlü sselanbieter stellt eine Secure Packager- und Encoder Key Exchange-API zur Bearbeitu ng eingehender Schlüssel anfragen zur Verfügung.	7. September 2021

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.