Partner- und Kundenleitfaden

Secure Packager and Encoder Key Exchange API-Spezifikation

Secure Packager and Encoder Key Exchange API-Spezifikation: Partner- und Kundenleitfaden

Table of Contents

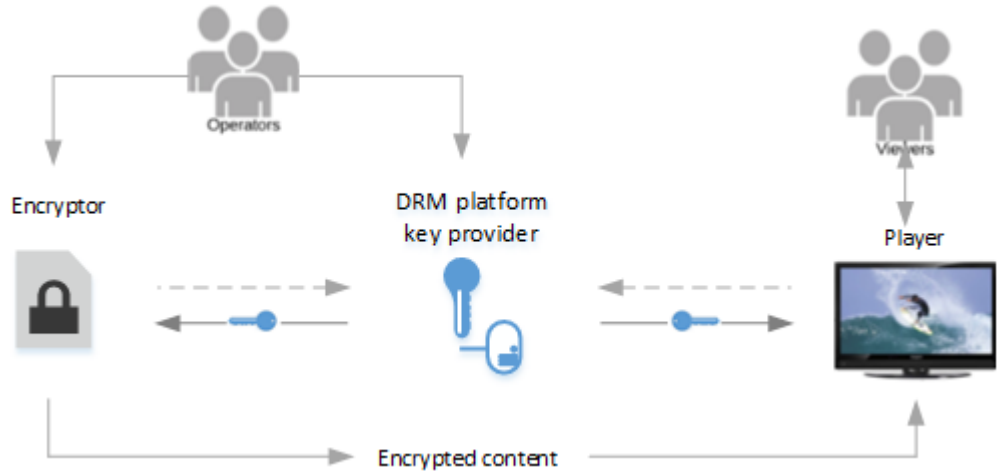
Was ist Secure Packager und Encoder Key Exchange?

Secure Packager und Encoder Key Exchange (SPEKE) definiert den Standard für die Kommunikation zwischen Verschlüsselungs- und Paketanbietern von Medieninhalten und DRM-Schlüsselanbietern (DRM). Die Spezifikation unterstützt Verschlüsseler, die lokal und in der AWS Cloud ausgeführt werden.

Themen

Allgemeine Architektur

Die folgende Abbildung zeigt eine allgemeine Ansicht der SPEKE-Inhaltsverschlüsselungsarchitektur für On-Premises-Produkte.



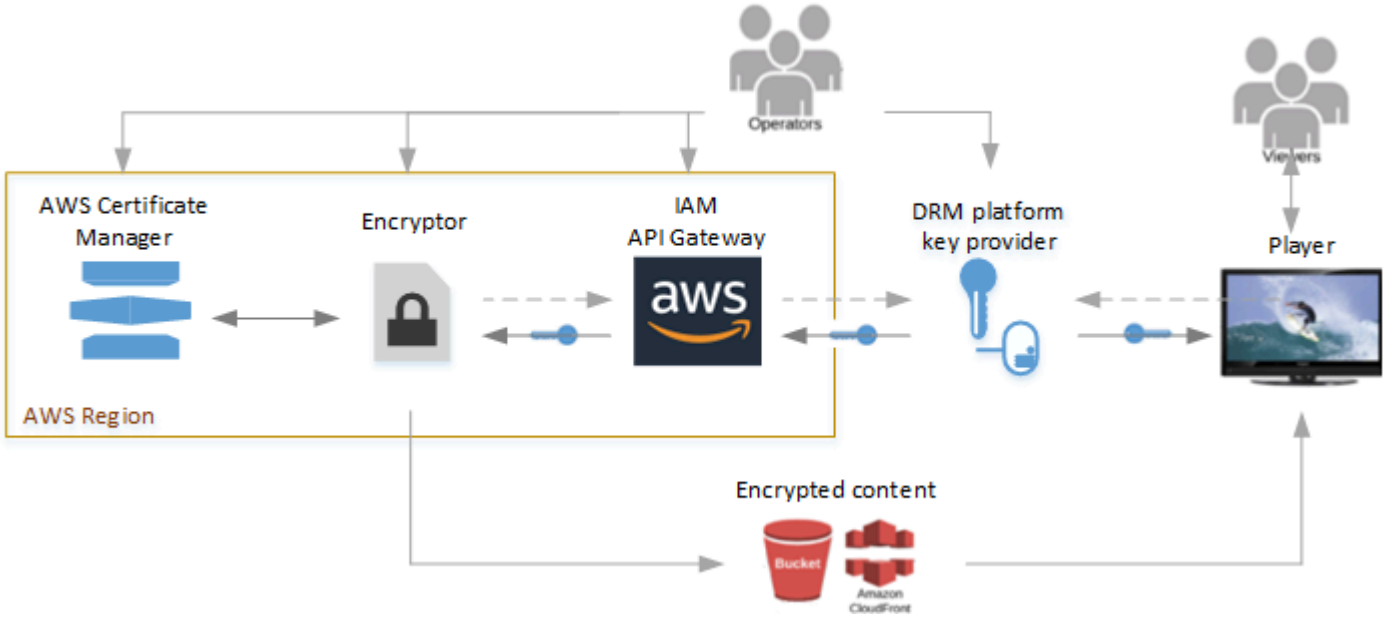
Dies sind die Hauptkomponenten der eben beschriebenen Architektur:

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

- Player – Fordert Schlüssel von demselben DRM-Plattformschlüsselanbieter an, den der Player verwendet, um den Inhalt zu entsperren und ihn seinen Zuschauern bereitzustellen.

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:

- Verschlüsselung – 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 stellt den verschlüsselten Inhalt in einem Amazon S3-Bucket oder über eine Amazon- CloudFront Verteilung bereit.
- AWS IAM und Amazon API Gateway – Verwaltet vom Kunden vertrauenswürdige Rollen und die Proxy-Kommunikation zwischen dem Verschlüsselung 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. Die API Gateway-API muss sich in der gleichen AWS-Region wie der Verschlüsseler befinden.
- AWS Certificate Manager – (Optional) Bietet Zertifikatverwaltung 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.

- DRM-Plattform-Schlüsselanbieter – Stellt Verschlüsselungsschlüssel für den Verschlüsseler über eine SPEKE-konforme API bereit. Der Anbieter stellt außerdem Media-Playern Lizenzen für die Entschlüsselung bereit.
- Player – Fordert Schlüssel von demselben DRM-Plattformschlüsselanbieter an, den der Player verwendet, um den Inhalt zu entsperren und ihn seinen Zuschauern bereitzustellen.

Erste Schritte

Weitere einführende Informationen zu SPEKE finden Sie unter Sind Sie noch nicht mit SPEKE vertraut?.

Sind Sie Kunde?

Nehmen Sie Kontakt mit einem AWS Elemental-DRM-Plattformanbieter auf, damit die Verwendung der Verschlüsselung eingerichtet werden kann. Weitere Informationen 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. Weitere Informationen finden Sie unter SPEKE-API-Spezifikation .

Sie sind noch nicht mit SPEKE vertraut?

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

Eine Einführung in SPEKE finden Sie im folgenden Webcast:

Verwandte Services und Spezifikationen

- API-Gateway-Berechtigungen – So steuern Sie den Zugriff auf eine API mit AWS Identity and Access Management (AWS IAM)-Berechtigungen.
- AWS AssumeRole – So verwenden Sie 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 Spezifikationsversion des DASH-IF Content Protection Information Exchange Format (CPIX), auf der diese SPEKE-v1.0-Spezifikation basiert.
- DASH-IF CPIX-Spezifikation v2.3 – Die Spezifikationsversion des DASH-IF Content Protection Information Exchange Format (CPIX), auf der diese SPEKE-v2.0-Spezifikation basiert.
- DASH-IF-System-IDs – Die Liste der registrierten Kennungen für DRM-Systeme.
- https://github.com/awslabs/speke-reference-server – Beispiel für einen Referenzschlüsselanbieter, der mit Ihrem AWS-Konto verwendet werden soll, 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 – Amazon-Ressourcenname. 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 stellt möglicherweise auch Quellmedien (Mezzanine-

Format zum Zweck der Transcodierung), Komponenten-IDs, Schlüssel-IDs (Key Identifiers, KIDs), Schlüsselwerte, Codierungsanweisungen und Metadaten zur Beschreibung der Inhalte bereit.

- DRM – Verwaltung digitaler Rechte. Wird verwendet, um urheberrechtlich geschützte digitale Inhalte vor nicht genehmigtem Zugriff zu schützen.
- DRM-Plattform – Ein System, das DRM-Funktionalität und -Unterstützung für Content Encryptors und Viewer bietet, einschließlich der Bereitstellung von DRM-Schlüsseln und der Lizenzierung für die Inhaltsverschlüsselung und -entschlüsselung.
- 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.
- Verschlüsselung – Eine Medienverarbeitungskomponente, die Medieninhalte mit 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 Verarbeitung von Schlüsselanforderungen bereitstellt. Der Schlüsselanbieter kann der Schlüsselserver selbst oder eine andere Komponente der Plattform sein.
- Schlüsselserver – Die Komponente einer DRM-Plattform, die Schlüssel für die Inhaltsverschlüsselung und -entschlüsselung verwaltet.
- Operator – Eine Person, die für den Betrieb des Gesamtsystems verantwortlich ist, einschließlich des Verschlüsselungs- und Schlüsselanbieters.
- Player – Ein Media Player, der im Namen eines Viewers 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

Schützen Sie Ihre Inhalte vor unbefugter Verwendung, indem Sie einen Secure Packager- und Encoder Key Exchange (SPEKE)-Schlüsselanbieter für die digitale Rechteverwaltung (DRM) mit Ihrem -Verschlüsselung und mit Ihren Media Playern kombinieren. SPEKE definiert den Standard für die Kommunikation zwischen Verschlüsselern und Paketern 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

Integrieren eines DRM-Plattformanbieters

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, verfügen derzeit über keine Amazon Partner Network-Seite, aber Sie können sie direkt kontaktieren. Die Partner können Ihnen bei der Einrichtung ihrer Plattformen helfen.

DRM-Plattformanbieter	Unterstützung für SPEKE v1	Unterstützung für SPEKE v2 (AWS Elemental MediaPackage)
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√

DRM-Plattformanbieter	Unterstützung für SPEKE v1	Unterstützung für SPEKE v2 (AWS Elemental MediaPackage)
INKA Entworks	√	√
Insys Cloud DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√
JW-Player	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	

SPEKE-Unterstützung in AWS-Services und -Produkten

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	Unterstützung für SPEKE v1	Unterstützung für SPEKE v2	Unterstützte DRM-Technologien
AWS Elemental MediaConvert – Service, der in der AWS Cloud ausgeführt wird	√		Dokumentation
AWS Elemental MediaPackage – Service, der in der AWS Cloud ausgeführt wird	√	√	Dokumentation
AWS Elemental Live – On-Premises-Produkt	√		Dokumentation: MPEG-DASH/HLS
AWS Elemental Server – On-Premises-Produkt	√		Dokumentation

SPEKE-Unterstützung in AWS-Partnerservices und -produkten

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	Unterstützung für SPEKE v1	Unterstützung für SPEKE v2	Unterstützte DRM-Technologien
Bitmovin-Live-Videokodierung	√		Dokumentation

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

SPEKE-API-Spezifikation

Dies ist die REST-API-Spezifikation für Secure Packager und 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 die Inhaltsschlüssel im Dokument auch für eine sicherere Verschlüsselung end-to-end verschlüsseln.

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.
- Unterstützung für HLS-, MSS- und DASH-Paketierung und ihre gängigen DRM-Systeme einschließen: FairPlay PlayReadyund Widevine/CENC.
- Einfachheit und Erweiterbarkeit der Spezifikation, um zukünftige DRM-Systeme unterstützen zu können.
- Verwendung einer einfachen REST API.

> **Note**
>
>

IN KEINEM FALL SIND DIE AUTOREN ODER COPYRIGHT-INHABER DIESES MATERIALS FÜR ANSPRÜCHE, HAFTUNGEN ODER ANDERE HAFTUNGEN VERANTWORTLICH, UNABHÄNGIG DAVON, OB ES SICH UM EINE VERTRAGSAKTION, EINE DELEGIERUNG ODER ANDERWEITIGE HAFTUNG HANDELT, DIE VON, AUS ODER IM ZUSAMMENHANG MIT DIESEM MATERIAL ODER DER VERWENDUNG ODER ANDEREN VORGEHENSWEISEN DIESES MATERIALS STAMMT.

Themen

Authentifizierung

SPEKE erfordert die Authentifizierung für On-Premises-Produkte und für Services und Funktionen, die in der AWS Cloud ausgeführt werden.

Themen

Authentifizierung für AWS Cloud-Implementierungen

SPEKE erfordert die AWS-Authentifizierung über IAM-Rollen für die Verwendung mit einem Verschlüsselung. 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 Operator 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 zum Erstellen einer Rolle finden Sie unter AWS AssumeRole. Weitere Informationen zum Signieren einer Anforderung finden Sie unter AWS Sigv4.

Authentifizierung für On-Premises-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 Autorisierungs-Header besteht aus der Kennung `Digest` gefolgt von einer Reihe von Werten, die die Anforderung authentifizieren. Insbesondere wird ein Antwortwert durch eine Reihe von MD5-Hash-Funktionen generiert, die einen eindeutigen, one-time-use einmaligen vom Server enthalten, der verwendet wird, um sicherzustellen, dass das Passwort sicher übertragen wird.
- Grundlegende Authentifizierung – Der Autorisierungs-Header 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

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.

Secure Packager und Encoder Key Exchange verwenden die Definition der Datenstruktur des DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) für den Schlüsselaustausch mit einigen Einschränkungen. DASH-IF-CPIX definiert ein Schema, um einen erweiterbaren, Multi-DRM-Austausch zwischen DRM-Plattform und Verschlüsseler zu ermöglichen. 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

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 digitale Signaturüberprüfung (XMLDSIG) für Anforderungs- oder Antwortnutzlasten.
  - SPEKE erfordert 2048 RSA-basierte Zertifikate.
- Für das Rotieren von Schlüssel-Workflows benötigt SPEKE den `ContentKeyUsageRule` Filter `KeyPeriodFilter`. SPEKE ignoriert alle anderen `ContentKeyUsageRule` Einstellungen.
- SPEKE lässt die `UpdateHistoryItemList` Funktionalität weg. Wenn die Liste in der Antwort vorhanden ist, ignoriert SPEKE sie.
- SPEKE unterstützt die Schlüsselrotation. SPEKE verwendet nur den Index `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-Wiedergabeliste stellt SPEKE unter dem -DRMSystemTag die optionalen benutzerdefinierten Parameter speke:KeyFormat und speke:KeyFormatVersionsfür die Werte der - KEYFORMAT und -KEYFORMATVERSIONSParameter des -EXT-X-KEYTags bereit.

  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 Spuren oder Schlüssel pro Inhalt.

  Der SPEKE-konforme Verschlüsselung fungiert als Client und sendet POST Operationen an den Schlüsselanbieter-Endpunkt. 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-Nutzlastkomponenten

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. Unter DASH-IF-System-IDs finden Sie eine Liste.
`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.

_Beispielanforderungen 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 Standardschlüssel 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 den Aufruf von Live-Workflow-Methoden

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-Nutzlastantwort
`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 Aufrufe von VOD-Workflow-Methoden

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 der 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 Verschlüsselung von Inhaltsschlüsseln gewährleistet vollen end-to-end Schutz, indem die Inhaltsschlüssel für die Übertragung verschlüsselt werden, zusätzlich zur Verschlüsselung des Inhalts selbst. Wenn Sie dies nicht für Ihren Schlüsselanbieter implementieren, verlassen Sie sich aus Sicherheitsgründen auf die Verschlüsselung der Transportebene plus die starke Authentifizierung.

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

Einschränkungen

SPEKE unterstützt die Verschlüsselung von Inhaltsschlüsseln, wie in der DASH-IF CPIX-Spezifikation angegeben, mit den folgenden Einschränkungen:

- SPEKE unterstützt keine digitale Signaturüberprüfung (XMLDSIG) für Anforderungs- oder Antwortnutzlasten.
- SPEKE erfordert 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 Schlüsselkennung

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

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.

Secure Packager und Encoder Key Exchange verwenden die Definition der Datenstruktur des DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) für den Schlüsselaustausch mit einigen Einschränkungen. DASH-IF-CPIX definiert ein Schema, um einen erweiterbaren, Multi-DRM-Austausch zwischen DRM-Plattform und Verschlüsseler zu ermöglichen. 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 Version 2.0 ist SPEKE auf eine bestimmte CPIX-Version abgestimmt:

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

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

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

- 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 werden durch ersetzt `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id` wird ersetzt durch `CPIX@contentId`
- Neue obligatorische CPIX-Attribute: `CPIX@version`, `ContentKey@commonEncryptionScheme`
- Neues optionales CPIX-Element: `DRMSystem.ContentProtectionData`
- Unterstützung für mehrere Inhaltsschlüssel

- Versionsübergreifender Mechanismus zwischen SPEKE und CPIX
- Entwicklung von HTTP-Headern: neuer `X-Speke-Version` Header, `Speke-User-Agent` Header in umbenannt `X-Speke-User-Agent`
- Veraltung der Heartbeat-API

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

Themen

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

Die Spezifikation des DASH Industry Forum CPIX 2.3 unterstützt eine Reihe von Anwendungsfällen und Topologien. Die Spezifikation SPEKE API v2.0 definiert sowohl ein CPIX-Profil als auch eine API für CPIX. Um diese beiden Ziele zu erreichen, entspricht sie der 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 digitale Signaturüberprüfung (XMLDSIG) für Anforderungs- oder Antwortnutzlasten.
  - SPEKE erfordert 2048 RSA-basierte Zertifikate.
- SPEKE nutzt nur eine Teilmenge der CPIX-Funktionen:

  - SPEKE lässt die `UpdateHistoryItemList` Funktionalität weg. Wenn die Liste in der Antwort vorhanden ist, ignoriert SPEKE sie.
  - SPEKE lässt die Stamm-/Blattschlüssel-Funktionalität weg. Wenn das `ContentKey@dependsOnKey` Attribut in der Antwort vorhanden ist, ignoriert SPEKE es.
  - SPEKE lässt das -`BitrateFilter`Element und das -`VideoFilter@wcg`Attribut weg. 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-Nutzlastkomponenten oder auf der Seite Verschlüsselungsvertrag als „unterstützt“ verwiesen wird, können in CPIX-Dokumenten verwendet werden, die mit SPEKE v2 ausgetauscht werden.
- Wenn sie vom Verschlüsselung in eine CPIX-Anforderung aufgenommen werden, müssen alle Elemente und Attribute einen gültigen Wert in der CPIX-Antwort des Schlüsselanbieters enthalten. Ist dies nicht der Fall, stoppt der Verschlüsselung 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 Verschlüsselung muss einen Wert für das `CPIX@contentId` Attribut enthalten. Wenn Sie einen leeren Wert für dieses Attribut erhalten, muss der Schlüsselanbieter einen Fehler mit der Beschreibung „Fehlende CPIX@contentId“ zurückgeben. Der `CPIX@contentId` Wert kann vom Schlüsselanbieter nicht überschrieben werden.

  `CPIX@id` -Wert, wenn nicht null, wird vom Schlüsselanbieter ignoriert.
- Der Verschlüsselung muss einen Wert für das `CPIX@version` Attribut enthalten. Wenn Sie einen leeren Wert für dieses Attribut erhalten, muss der Schlüsselanbieter einen Fehler mit der Beschreibung „Fehlende CPIX@Version“ zurückgeben. Wenn Sie eine Anforderung mit

einer nicht unterstützten Version erhalten, lautet die vom Schlüsselanbieter zurückgegebene Fehlerbeschreibung „Nicht unterstützte CPIX@Version“.

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

- Der Verschlüsselung muss einen Wert für das `ContentKey@commonEncryptionScheme` Attribut für jeden angeforderten Schlüssel enthalten. Wenn Sie einen leeren Wert für dieses Attribut erhalten, muss der Schlüsselanbieter einen Fehler mit der Beschreibung „Missing ContentKey@commonEncryptionScheme for KID`id`“ zurückgeben.

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

  Nicht alle `ContentKey@commonEncryptionScheme` Werte sind mit allen DRM-Technologien kompatibel. Wenn der Schlüsselanbieter eine solche Kombination erhält, muss er einen Fehler mit der Beschreibung „ContentKey@commonEncryptionScheme non compatible with DRMSystem`id`“ zurückgeben.

  `ContentKey@commonEncryptionScheme` Der -Wert kann vom Schlüsselanbieter nicht überschrieben werden.
- Beim Empfang unterschiedlicher Werte für `DRMSystem@PSSH` und `DRMSystem.ContentProtectionData` innerXML<pssh>Element im CPIX-Antworttext muss der Verschlüsselung angehalten und ein Fehler ausgegeben werden.

API für CPIX

- Der Schlüsselanbieter muss einen Wert für den `X-Speke-User-Agent` HTTP-Antwort-Header enthalten.
- Ein SPEKE-konformer Verschlüsselung fungiert als Client und sendet POST-Operationen an den Schlüsselanbieter-Endpunkt.
- Der Verschlüsseler muss einen Wert für den `X-Speke-Version` HTTP-Anforderungs-Header enthalten, wobei die SPEKE-Version, die mit der Anforderung verwendet wird, als MajorVersion., MinorVersionwie „2.0“ für SPEKE v2.0 festgelegt ist. Wenn der Schlüsselanbieter die vom Verschlüsselung für die aktuelle Anforderung verwendete SPEKE-Version nicht unterstützt, muss der Schlüsselanbieter einen Fehler mit der Beschreibung „Nicht unterstützte SPEKE-Version“ zurückgeben und nicht versuchen, das CPIX-Dokument nach bestem Bemühen zu verarbeiten.

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

- Beim Empfang von Fehlern im Antworttext muss der Verschlüsselung einen Fehler ausgeben und die Anforderung nicht mit einer SPEKE v1.0-Versionsverwaltung wiederholen.

  Wenn der Schlüsselanbieter keinen Fehler zurückgibt, aber kein CPIX-Dokument zurückgibt, das die obligatorischen Informationen enthält, sollte der Verschlüsselungsdienst angehalten und ein Fehler ausgegeben werden.

Die folgende Tabelle fasst die Standardnachrichten zusammen, die vom Schlüsselanbieter im Nachrichtentext zurückgegeben werden müssen. Der HTTP-Antwortcode darf in Fehlerfällen 4XX oder 5XX sein, niemals 200. Der Fehlercode 422 kann für alle Fehler im Zusammenhang mit SPEKE/CPIX verwendet werden.

Fehlerfall	Fehlermeldung
CPIX@contentId ist nicht definiert	Fehlende CPIX@contentId
CPIX@Version ist nicht definiert	Fehlende CPIX@Version
CPIX@Version wird nicht unterstützt	Nicht unterstützte CPIX@Version
ContentKey@ commonEncryptionScheme ist nicht definiert	Fehlende ContentKey@commonEncryption Scheme für KID `id` (wobei gleich ContentKe y@kid-Wert `id` ist)
Mehrere ContentKey@commonEncryption Scheme values, die in einem einzigen CPIX-Dokument verwendet werden	Nicht konforme ContentKey@commonE ncryptionScheme Kombination
ContentKey@ commonEncryptionScheme ist nicht mit der DRM-Technologie kompatibel	ContentKey@commonEncryptionScheme nicht kompatibel mit DRMSystem `id` (wobei gleich DRMSystem @systemId-Wert `id` ist)
Der X-Speke-Version-Header-Wert ist keine unterstützte SPEKE-Version	Nicht unterstützte SPEKE-Version

Fehlerfall	Fehlermeldung
Der Verschlüsselungsvertrag ist falsch formatiert	Falsch formatierter Verschlüsselungsvertrag
Der Verschlüsselungsvertrag unterliegt DRM-Sicherheitseinschränkungen	Angeforderter CPIX-Verschlüsselungsvertrag wird nicht unterstützt
Der Verschlüsselungsvertrag enthält kein - VideoFilter oder - AudioFilter Element	Fehlender CPIX-Verschlüsselungsvertrag

SPEKE API v2 – Standard-Nutzlastkomponenten

Durch eine einzelne SPEKE-Anforderung kann der Verschlüsselung mehrere Inhaltsschlüssel zusammen mit der erforderlichen Manfest-Signalisierung für mehrere Verpackungsformate gemäß dem Verschlüsselungsvertrag anfordern, der für einen bestimmten Inhalt definiert ist.

Um all diese Aspekte abzudecken, besteht ein CPIX-Standarddokument aus drei obligatorischen Listenabschnitten sowie einem optionalen Listenabschnitt für die Rotation von Live-Inhaltsschlüsseln.

<cpix:ContentKeyList>-Abschnitt und oberstes <cpix:CPIX>-Element

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

Gemäß der CPIX-Spezifikation sind die möglichen Werte des `ContentKey@commonEncryptionScheme` Attributs in der Spezifikation Gemeinsame Verschlüsselung in ISO-Basismediendateidateien (ISO/IEC 23001-7:2016) definiert:

- 'cenc': AES-CTR-Modus Vollbeispiel und Video-NAL-Subsample-Verschlüsselung
- 'cbc1': AES-CBC-Modus Vollbeispiel- und Video-NAL-Subsample-Verschlüsselung
- „Zense“: AES-CTR-Modus teilweise Video-NAL-Musterverschlüsselung
- 'cbcs': AES-CBC-Modus partielle Video-NAL-Musterverschlüsselung

Das folgende Beispiel zeigt ein CPIX-Dokument mit einem einzelnen, nicht verschlüsselten 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 werden Inhaltsschlüssel nicht verschlüsselt, wie im folgenden Beispiel. Die Verschlüsselung von Inhaltsschlüsseln kann jedoch vom Verschlüsseler durch die Aufnahme des Elements <cpix:DeliveryDataList> angefordert werden. Weitere Informationen finden Sie im Abschnitt Verschlüsselung von Inhaltsschlüsseln.

Von SPEKE unterstütztes Element	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix:CPIX>	contentId , Version, xmlns:cpix, xmlns:pskc	Name, xmlns:enc	Ein <cpix:ContentKeyList>, ein <cpix:DRMSystemList>, ein <cpix:ContentKeyUsageRuleList>	ein <cpix:DeliveryDataList>, ein <cpix:ContentKeyPeriodList>
<cpix:ContentKeyList>	-	id	mindestens ein <cpix:ContentKey>	-
<cpix:ContentKey>	kid, commonEncryptionScheme, Daten	id, Algorithmus, explicitIV	ein <pskc:Secret>	-

Von SPEKE unterstütztes Element	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<pskc:Secret>	PlainValue oder EncryptedValue	ValueMAC	-	<enc:EncryptionMethod>, <enc:CipherData>

<cpix:DRM SystemList> Abschnitt

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

Das folgende Beispiel zeigt eine DRM-Systemliste mit einer einzelnen 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 DRMsystemIDs finden Sie im Abschnitt Inhaltsschutz des DASH-IF-Identifiers-Repositorys.

Von SPEKE unterstütztes Element	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix:DRM SystemList>	-	id	mindestens ein <cpix:DRM System >	-
<cpix:DRM System >	kid, systemId	ID, Name, PSSH	-	ContentPr otectionData, SmoothStr eamingPro tectionHe aderData, zwei <cpix:HLS SignalingData>-Elemente mit unterschi edlichem Wiedergab elistenattributwer t

`DRMSystem@PSSH` ist obligatorisch, wenn die ISO-BMFF-Kapselung auf Mediensegmente angewendet wird. Das `DRMSystem.ContentProtectionData` Element innerXML `<pssh>` wird vom Verschlüsselung nur für Manifest-Signalisierungszwecke genutzt.

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

Wenn die `DRMSystem` Signalisierung in HLS-Manifesten übertragen werden soll, müssen sowohl ein - als auch `<cpix:HLSSignalingData playlist="media">` ein -`<cpix:HLSSignalingData playlist="master">`Element in die CPIX-Anforderung und -Antwort aufgenommen werden.

<cpix:ContentKeyPeriodList>-Abschnitt

Dies ist ein optionaler Abschnitt, der nur für Live-Streaming relevant ist und die auf den Inhalt angewendeten Krypto-Zeiträume definiert.

Das -<cpix:ContentKeyPeriodList>Element kann ein oder mehrere <cpix:ContentKeyPeriod> untergeordnete Elemente enthalten, die jeweils einen unterschiedlichen Kryptozeitraum in der Live-Zeitleiste beschreiben. Die Verwendung von 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>
```

Von SPEKE unterstütztes Element	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix:ContentKeyPeriodList>	-	id	mindestens ein <cpix:ContentKeyPeriod>	-
<cpix:ContentKeyPeriod>	ID, Index	-	-	-

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

Abschnitt <cpix:ContentKeyUsageRuleList>

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

Das Element <cpix:ContentKeyUsageRuleList> kann ein oder mehrere untergeordnete Elemente <cpix:ContentKeyUsageRule> enthalten, die jeweils die Spuren beschreiben, auf die ein bestimmter Inhaltsschlüssel vom Verschlüsselungsdienst angewendet wird, möglicherweise während eines bestimmten Kryptozeitraums. Mindestens ein <cpix:AudioFilter>- oder ein <cpix:VideoFilter>-Element muss in einem <cpix:ContentKeyUsageRule>-Element vorhanden sein.

Das folgende Beispiel zeigt eine einfache Liste mit nur einer Regel, die während eines bestimmten Kryptozeitraums einen einzelnen Inhaltsschlüssel auf alle Audio- und Videospuren 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>
```

Von SPEKE unterstütztes Element	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix:ContentKeyUsageRuleList>	-	id	mindestens ein <cpix:ContentKeyUsageRule>	-
<cpix:ContentKeyUsageRule>	KID, intendedTrackType	-	mindestens ein <cpix:AudioFilter> oder ein <cpix:VideoFilter> (*)	<cpix:KeyPeriodFilter>
<cpix:KeyPeriodFilter>	periodId	-	-	-
<cpix:AudioFilter>	-	minChannels ,maxChannels	-	-
<cpix:VideoFilter>	-	minPixels, maxPixels, hdr, minFps , maxFps	-	-

(*) Eine ausführliche Erklärung zur Verwendung einzelner oder mehrerer Inhaltsschlüssel zum Schutz eines oder mehrerer Spuren in einem Streamset finden Sie im Abschnitt Dokumentation zur Verschlüsselungsdokumentation._

SPEKE API v2 – Verschlüsselungsvertrag

Der Verschlüsselungsvertrag definiert, welche Inhaltsschlüssel schützen, welche Spuren in einem bestimmten Streamset basierend auf den Spurenmerkmalen.

Die Verwendung mehrerer Inhaltsschlüssel für verschiedene Spuren in einem Streamset ist – obwohl es sich um eine empfohlene bewährte Methode in der Branche handelt – nicht obligatorisch, sondern wird empfohlen – mindestens zwei verschiedene Inhaltsschlüssel, einen für Audiospuren und einen für Videospuren. Die Verwendung eines einzelnen Inhaltsschlüssels zum Verschlüsseln mehrerer Spuren ist möglich, muss jedoch explizit in dem CPIX-Dokument signalisiert werden, das vom Verschlüsseler an den Schlüsselanbieter gesendet wird. Im Allgemeinen beschreibt der Verschlüsselung immer genau, wie viele Inhaltsschlüssel erforderlich sind und wie sie zur Verschlüsselung der verschiedenen Medienpfade genutzt werden.

Prinzipien

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

Die Regeln für diese Beziehung sind die folgenden:

- Wenn alle Audio- und Videospuren 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 diesem Fall müssen sowohl ein als auch `<cpix:AudioFilter />` ein `<cpix:VideoFilter />` untergeordnetes Element ohne

Attribut enthalten sein. Jede andere Kombination von - `<cpix:AudioFilter>` und/oder -`<cpix:VideoFilter>`Elementen ist in diesem bestimmten Kontext ungültig.

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

Filter

CPIX definiert mehrere Filterelemente und Attribute, aber SPEKE unterstützt nur eine Teilmenge davon. In der folgenden Tabelle sind diese Unterschiede zusammengefasst:

CPIX-Filtertyp	Gesamte SPEKE-Unterstützung	Von SPEKE unterstützte Filterattribute	Filterattribute, die von SPEKE nicht unterstützt werden
<cpix:VideoFilter>	Ja	minPixels , maxPixels , hdr, minFps , maxFps (optionale Attribute)	wcg
<cpix:AudioFilter>	Ja	minChannels , maxChannels (optionale Attribute)	
<cpix:KeyPeriodFilter>	Ja	periodId (Verzeichnisattribut)	
<cpix:BitrateFilter>	Nein	N/A	N/A

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

Gemäß der CPIX-Spezifikation für ist VideoFilter[minPixels ,maxPixels] ein vollständig inklusiver Bereich in beiden Dimensionen, während (minFps , maxFps] nur für die maxFps-Dimension inklusive ist. Für ist AudioFilter[minChannels ,maxChannels] ein inklusiver Bereich in beiden Dimensionen.

Problematische Situationen

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

In dieser Situation	Der Verschlüsseler sollte/shall ...	Der Schlüsselanbieter sollte/shall ...
Es gilt keine Regel für einen oder mehrere Tracks im Streamset (siehe Beispiel 3 unten).	Der Verschlüsseler sollte sich seine Konfiguration ansehen (außerhalb der CPIX-Nutzlast) und überprüfen, ob die betroffenen Spuren keine Verschlüsselung erfordern. Wenn dies nicht erwartet wird, sollte der Verschlüsselung einen Fehler auslösen und die Verarbeitung beenden.	Nicht relevant: Der Schlüsselanbieter verfügt nicht über Kenntnisse der Streamset-Struktur.
Mehrere Regeln überschneiden sich und schlagen mehrere Inhaltsschlüssel vor, um einen bestimmten Track zu verschlüsseln	Der Verschlüsseler sollte den zuletzt ContentKeyUsageRule erfolgreich ausgewerteten in der Reihenfolge des Dokuments anwenden.	Nicht relevant: Der Schlüsselanbieter verfügt nicht über Kenntnisse der Streamset-Struktur.

In dieser Situation	Der Verschlüsseler sollte/shall ...	Der Schlüsselanbieter sollte/shall ...
Der Verschlüsselungsvertrag ändert sich in einem einzigen SPEKE-Anforderungs-/Antwortzyklus	Der Verschlüsseler muss eine Ausnahme auslösen und die Verarbeitung beenden, da der Schlüsselanbieter nicht für die Definition des Verschlüsselungsvertrags verantwortlich ist.	Um zu verhindern, dass diese Situation von vornherein eintritt, darf der Schlüsselanbieter keinen Verschlüsselungsvertrag ändern, der in der CPIX-Nutzlast der SPEKE-Anforderung empfangen wurde.
Fehlgeformter Verschlüsselungsvertrag: Ausnahme der Kardinalitätsbeschränkung intendedTrackType/Filter, nicht unterstützte Filter oder Attribute	Der Verschlüsselung muss eine Ausnahme auslösen, die Verarbeitung beenden und die SPEKE-Anforderung nicht an den Schlüsselanbieter senden, da dies höchstwahrscheinlich zu fehlerhaftem Inhaltsschutz führen würde oder einige Spuren ungeschützt lassen würde.	Der Schlüsselanbieter muss eine Ausnahme auslösen und den Fehler „Malformierter Verschlüsselungsvertrag“ zurückgeben.
Wellform-Verschlüsselungsvertrag, aber unter Verletzung der DRM-Sicherheitsstufenbeschränkungen: Beispielsweise wird ein einzelner Inhaltsschlüssel angefordert, um sowohl Audiospuren als auch UHD-Videospuren zu schützen	Wenn der Verschlüsseler über Kenntnisse der DRM-Sicherheitsstufenbeschränkungen verfügt, sollte er eine Ausnahme auslösen, die Verarbeitung beenden und die SPEKE-Anfrage nicht an den Schlüsselanbieter senden, da dies höchstwahrscheinlich zu fehlerhaftem Inhaltsschutz führen würde.	Der Schlüsselanbieter muss eine Ausnahme auslösen und den Fehler „Angeforderter CPIX-Verschlüsselungsvertrag wird nicht unterstützt“ zurückgeben.

In dieser Situation	Der Verschlüsseler sollte/shall ...	Der Schlüsselanbieter sollte/shall ...
Fehlender Verschlüsselungsvertrag	Der Verschlüsseler darf keine CPIX-Dokumente senden, die kein - VideoFilter oder - AudioFilter Element enthalten.	Der Schlüsselanbieter muss eine Ausnahme auslösen und den Fehler „Fehlender CPIX-Verschlüsselungsvertrag“ zurückgeben.

Beispiele für Verschlüsselungsverfahren

Beispiel 1: Ein Inhaltsschlüssel für alle Audio- und Videospuren

```
<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: ein Inhaltsschlüssel für alle Videospuren, mehrere Inhaltsschlüssel 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 Inhaltsschlüssel für alle Videospuren, mehrere Inhaltsschlüssel 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 den Aufruf von Live-Workflow-Methoden

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 Anforderu

Name	Typ	Auftreten	Beschreibung
			ng verwendet wird, als MajorVersion.Minor Version, 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 Anforderung verwendet wird, als MajorVersion.Minor Version, 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 der Inhaltsschlüsselverschlüsselung finden Sie unter Inhaltsschlüsselverschlüsselung.

Beispiel für eine Live-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Live-Anforderungsnutzlast vom Verschlüsselung zum 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 vom DRM-Schlüsselanbieter (zu Lesbarkeit wurden zurückgegebene Werte 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 Aufrufe von VOD-Workflow-Methoden

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 Anforderung verwendet wird, als MajorVersion.Minor

Name	Typ	Auftreten	Beschreibung
			Version, 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 Anforderung verwendet wird, 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 der Inhaltsschlüsselverschlüsselung finden Sie unter Inhaltsschlüsselverschlüsselung.

Beispiel für eine VOD-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische VOD-Anforderungsnutzlast vom Verschlüsselung zum 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 Antwortnutzlast vom DRM-Schlüsselanbieter (zu Lesbarkeit wurden zurückgegebene Werte 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 – Inhaltsschlüsselverschlüsselung

Sie können Ihrer SPEKE-Implementierung optional eine Inhaltsschlüsselverschlüsselung hinzufügen. Die Verschlüsselung von Inhaltsschlüsseln gewährleistet vollen end-to-end Schutz, indem die Inhaltsschlüssel für die Übertragung verschlüsselt werden, zusätzlich zur Verschlüsselung des Inhalts

selbst. Wenn Sie dies nicht für Ihren Schlüsselanbieter implementieren, verlassen Sie sich aus Sicherheitsgründen auf die Verschlüsselung der Transportebene plus die starke Authentifizierung.

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

Einschränkungen

SPEKE unterstützt die Verschlüsselung von Inhaltsschlüsseln, wie in der DASH-IF CPIX-Spezifikation angegeben, mit den folgenden Einschränkungen:

- SPEKE unterstützt keine digitale Signaturüberprüfung (XMLDSIG) für Anforderungs- oder Antwortnutzlasten.
- SPEKE erfordert 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 Spezifikation DASH-IF CPIX 2.3.

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 Schlüsselkennung

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>
```

License

National Commons Attribution-ShareAlike 4.0 Internationale öffentliche Lizenz

Indem Sie sich mit den Telefonierechten (wie unten definiert) befassen, akzeptieren Sie die Geschäftsbedingungen dieser Bol 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 des Adapters bezeichnet die Lizenz, die Sie auf Ihr Copyright und ähnliche Rechte in Ihren Beiträgen zu angepasstem Material gemäß den Bedingungen dieser öffentlichen Lizenz anwenden.

c. BY-SA-kompatible Lizenz bezeichnet eine Lizenz, die unter creativecommons.org/compatiblelicenses, aufgeführt ist und von Bol Commons als im Wesentlichen Äquivalent dieser öffentlichen Lizenz 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 bezeichnet die Lizenzattribute, die im Namen einer Bol Commons Public License aufgeführt sind. Die Lizenzelemente dieser öffentlichen Lizenz sind Attribution 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. reproduzieren und teilen Sie das microSD-Material ganz oder teilweise; und

   B. produzieren, reproduzieren und teilen Sie angepasstes Material.

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 aus dem Telefonie – Adaptiertes Material. Jeder Empfänger von Adapted Material von Sie erhält automatisch ein Angebot von , um die Rechte im Adapted

Material unter den Bedingungen der von Ihnen angewendeten Lizenz des Adapters anzuwenden.

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. Moralische Rechte, z. B. das Recht der Integrität, werden unter dieser öffentlichen Lizenz nicht lizenziert. Das gilt auch für Publizität, Privatsphäre und/oder andere vergleichbare Persönlichkeitsrechte. Jedoch verzichtet der Lizenzgeber in dem Umfang auf solche Rechte des Lizenzgebers und/oder verpflichtet sich, solche Rechte in dem Umfang nicht geltend zu machen, der erforderlich ist, damit Sie die lizenzierten Rechte ausüben können. Im Übrigen bleiben die Rechte vorbehalten.
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. Behalten Sie Folgendes bei, wenn es von der Arzt mit dem Telefoniematerial bereitgestellt 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 Telefoniematerial geändert haben, und geben Sie an, ob Sie vorherige Änderungen angezeigt haben; und

C. geben an, dass das Telefoniematerial unter dieser öffentlichen Lizenz lizenziert ist, und fügen Sie den Text dieser öffentlichen Lizenz oder den URI oder Hyperlink zu dieser öffentlichen Lizenz ein.

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 angepasstes Material freigeben, das Sie produzieren, gelten zusätzlich zu den Bedingungen in Abschnitt 3(a) auch die folgenden Bedingungen.

1. Die von Ihnen angewendete Lizenz des Adapters muss eine Bol Commons-Lizenz mit denselben Lizenzelementen, dieser Version oder höher oder einer BY-SA-kompatiblen Lizenz sein.
2. Sie müssen den Text oder den URI oder Hyperlink auf die Lizenz des Adapters einfügen, die Sie anwenden. Sie können diese Bedingung auf angemessene Weise erfüllen, basierend auf dem Medium, den Mitteln und dem Kontext, in dem Sie angepasstes Material teilen.
3. Sie dürfen keine zusätzlichen oder unterschiedlichen Bedingungen oder Bedingungen für angepasstes Material anbieten oder festlegen oder effektive technische Maßnahmen

anwenden, die die Ausführung der im Rahmen der von Ihnen angewendeten Lizenz des Adapters gewährten Rechte einschränken.

Abschnitt 4: Datenbankherstellerrechte.

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

a. Um Defizite zu vermeiden, gewährt Ihnen Abschnitt 2 (a) das Recht, den gesamten Inhalt der Datenbank oder einen wesentlichen Teil davon zu extrahieren, wiederzuverwenden, zu reproduzieren und freizugeben;
b. Wenn Sie den gesamten oder einen wesentlichen Teil des Datenbankinhalts in eine Datenbank aufnehmen, in der Sie über Sui-Genris-Datenbankrechte verfügen, ist die Datenbank, in der Sie über Sui-Genris-Datenbankrechte verfügen (aber nicht über ihren individuellen Inhalt), angepasstes Material, auch für 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 zum Datum der Verletzung, vorausgesetzt, sie wird innerhalb von 30 Tagen nach Ihrer Entdeckung des Verstoßes behoben; oder

   2. bei ausdrücklicher Wiedereinsetzung durch den Arzt.

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.

Dokumentverlauf

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

SPEKE v1

Änderung	Beschreibung	Datum
Support-Matrix: AWS-Partnerservices und -produkte	Es wurde ein neuer Abschnitt für den SPEKE-Support in AWS-Partnerservices und -produkten hinzugefügt, in dem Bitmovin-Services aufgeführt sind.	13. Januar 2023
Updates für DRM-Plattformanbieter	Es wurden Links und neue Partnerinformationen zur DRM-Plattformanbieterliste hinzugefügt.	24. Januar 2019
Drittanbieter-Verschlüsseler einschließen	Architektur und Beschreibungen wurden aktualisiert, um Drittanbieter-Verschlüsseler zu berücksichtigen.	20. November 2018
Inhaltsschlüssel-Verschlüsselung	Hinzufügung der Option für die Verschlüsselung von Inhaltsschlüsseln. Zuvor unterstützten Secure Packager und Encoder Key Exchange nur die Bereitstellung von Klarschlüsseln.	30. Oktober 2018
Support-Matrix – AWS Elemental Live	Hinzufügung einer AWS Elemental Live-Unterstützungsmatrix.	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	Korrigierte Links zur DASH-IF-Website für die CPIX-Spez ifikation und die Seite für System-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 Veröffentlichung von Secure Packager und Encoder Key Exchange (SPEKE) Version 1, einer Spezifikation für die Kommunikation zwischen einem Content Encryptor und einem DRM-Schlüsselanbieter. Der DRM-Schlüsselanbieter stellt eine Secure Packager- und Encoder Key Exchange-API bereit, um eingehende Schlüsselanforderungen zu verarbeiten.	27. November 2017

SPEKE v2

Änderung	Beschreibung	Datum
Aktualisierungen des Abschnitts für DRM-Plattformanbieter	Der Spalte SPEKE v2 der Liste der DRM-Plattformanbieter wurden neue qualifizierte Partner hinzugefügt.	9. August 2023
Aktualisierungen der Beispiele für Aufrufe von Live- und VOD-Workflow-Methoden	Fehlender X-Speke-Version-Antwort-Header in den Abschnitten SPEKE v2 Live und VOD-Workflow-Methodenaufrufbeispiele hinzugefügt.	13. Januar 2023
Aktualisierungen der DRM-Plattformanbieter und des Abschnitts Verschlüsselungsvertrag	Der Spalte SPEKE v2 der Liste der DRM-Plattformanbieter wurden neue qualifizierte Partner hinzugefügt. Es	27. Januar 2022

Änderung	Beschreibung	Datum
	wurden zwei neue Beispiele für Verschlüsselungsve reinbarungen hinzugefügt und die maximale SD-Auflösung in allen betroffenen Beispielen auf 1024x576 geändert.	
Erstversion	Erste Veröffentlichung von Secure Packager und Encoder Key Exchange (SPEKE) Version 2.0, einer Spezifika tion für die Kommunikation zwischen einem Content Encryptor und einem DRM-Schlüsselanbieter. Der DRM-Schlüsselanbieter stellt eine Secure Packager- und Encoder Key Exchange-API bereit, um eingehende Schlüsselanforderungen zu verarbeiten.	7. September 2021

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.