Leitfaden für Partner und Kunden

Spezifikation für Secure Packager und Encoder Key Exchange API

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

Table of Contents

Was ist Secure Packager und Encoder Key Exchange? 1
Allgemeine Architektur 1
AWSCloud-basierte Architektur 2
Erste Schritte 3
Neu bei SPEKE? 4
Verwandte Serviceinformationen und Spezifikationen 4
Terminologie 4
Kunden-Onboarding 6
Beginnen Sie mit einem DRM Plattformanbieter 6
SPEKEUnterstützung bei Dienstleistungen und Produkten AWS 7
SPEKEUnterstützung bei AWS Partnerdienstleistungen und -produkten 8
SPEKEAPISpezifikation 9
Authentifizierung erforderlich für SPEKE 10
Authentifizierung für AWS Cloud-Implementierungen 10
Authentifizierung für lokale Produkte 11
SPEKEAPIv1 12
SPEKEAPIv1 — Anpassungen und Einschränkungen der -IF-Spezifikation DASH 13
SPEKEAPIv1 — Standard-Payload-Komponenten 14
SPEKEAPIv1 — Beispiele für Live-Workflow-Methodenaufrufe 17
SPEKEAPIv1 — Beispiele für VOD Workflow-Methodenaufrufe 22
SPEKEAPIv1 — Verschlüsselung von Inhaltsschlüsseln 25
SPEKEAPIv1 — Heartbeat 29
SPEKEAPIv1 — Überschreiben der Schlüssel-ID 30
SPEKEAPIv2 31
SPEKEAPIv2 — Anpassungen und Einschränkungen der -IF-Spezifikation DASH 33
SPEKEAPIv2 — Standard-Payload-Komponenten 37
SPEKEAPIv2 - Verschlüsselungsvertrag 43
SPEKEAPIv2 — Beispiele für Live-Workflow-Methodenaufrufe 53
SPEKEAPIv2 — Beispiele für VOD Workflow-Methodenaufrufe 59
SPEKEAPIv2 — Verschlüsselung von Inhaltsschlüsseln 64
SPEKEAPIv2 — Überschreiben der Schlüssel-ID 68
Lizenz für die Spezifikation SPEKE API 70
Creative Commons Namensnennung — ShareAlike 4.0 Internationale öffentliche Lizenz 70
Dokumentverlauf 78

..... lxxxii

Was ist Secure Packager und Encoder Key Exchange?

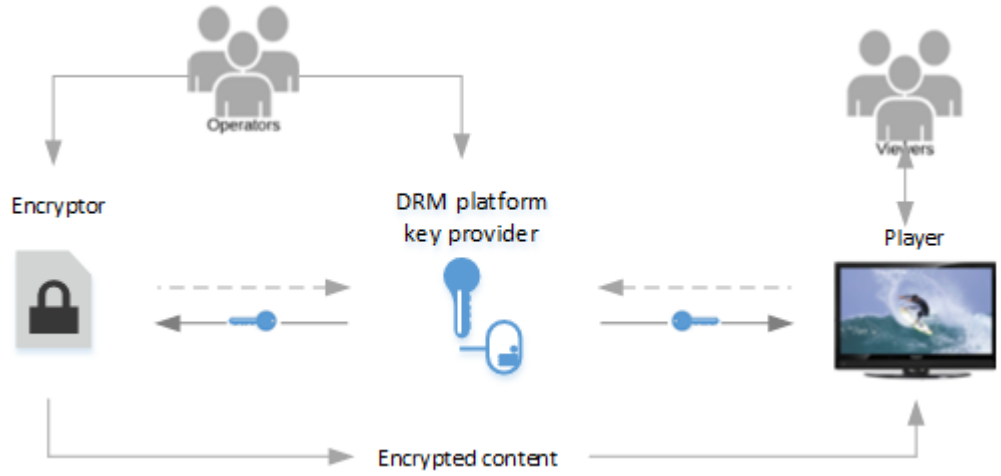
Secure Packager and Encoder Key Exchange (SPEKE) definiert den Standard für die Kommunikation zwischen Verschlüsselern und Paketierern von Medieninhalten und Schlüsselanbietern für die Verwaltung digitaler Rechte (). DRM Die Spezifikation berücksichtigt Verschlüsselungsprogramme, die vor Ort und in der Cloud ausgeführt werden. AWS

Themen

- Allgemeine Architektur
- AWSCloud-basierte Architektur
- Erste Schritte

Allgemeine Architektur

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



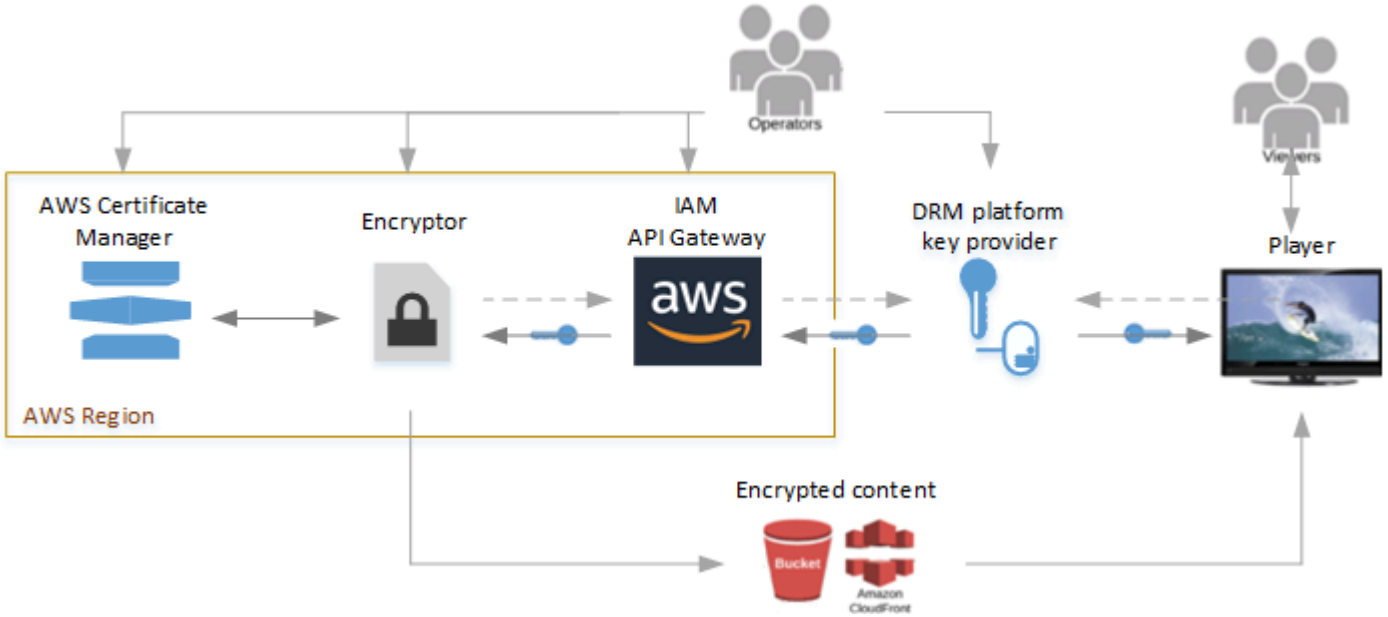
Dies sind die Hauptkomponenten der eben beschriebenen Architektur:

- Encryptor — Stellt die Verschlüsselungstechnologie bereit. Empfängt Verschlüsselungsanfragen von seinem Betreiber und ruft die erforderlichen Schlüssel vom DRM Schlüsselanbieter ab, um den verschlüsselten Inhalt zu sichern.
- DRMPlattform-Schlüsselanbieter — Stellt dem Verschlüsseler Verschlüsselungsschlüssel über eine SPEKE -konforme Schnittstelle zur Verfügung. API Der Anbieter stellt außerdem Media-Playern Lizenzen für die Entschlüsselung bereit.

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

AWSCloud-basierte Architektur

Die folgende Abbildung zeigt die High-Level-Architektur, wenn sie mit Diensten und Funktionen verwendet SPEKE wird, die in der AWS Cloud ausgeführt werden.



Dies sind die Hauptservices und -komponenten:

- Encryptor — Stellt die Verschlüsselungstechnologie in der AWS Cloud bereit. Der Verschlüsseler erhält Anfragen von seinem Betreiber und ruft über Amazon API Gateway die erforderlichen Verschlüsselungsschlüssel vom DRM Schlüsselanbieter ab, um den verschlüsselten Inhalt zu sichern. Es liefert den verschlüsselten Inhalt an einen Amazon S3 S3-Bucket oder über eine CloudFront Amazon-Distribution.
- AWSIAMund Amazon API Gateway — Verwaltet Rollen, denen Kunden vertrauen, und die Proxykommunikation zwischen dem Verschlüsseler und dem Schlüsselanbieter. APIGateway bietet Protokollierungsfunktionen und ermöglicht es Kunden, ihre Beziehungen zum Verschlüsseler und zur Plattform zu kontrollieren. DRM Kunden ermöglichen den Zugriff auf wichtige Anbieter über die IAM Rollenkonfiguration. APIDas Gateway muss sich in derselben AWS Region wie der Verschlüsseler befinden.
- AWSCertificate Manager — (Optional) Stellt die Zertifikatsverwaltung für die Inhaltsschlüsselverschlüsselung bereit. Die Verschlüsselung von Inhaltsschlüsseln ist das

empfohlene Verfahren, um die Kommunikation zu sichern. Der Zertifikatsmanager muss sich in derselben AWS Region wie der Verschlüsseler befinden.

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

Erste Schritte

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

Sind Sie Kunde?

Arbeiten Sie mit einem DRM Plattformanbieter von AWS Elemental zusammen, um die Verwendung von Verschlüsselung einzurichten. Einzelheiten finden Sie unter Kunden-Onboarding.

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

Stellen Sie Ihrem Schlüsselanbieter einen REST API gemäß der SPEKE Spezifikation zur Verfügung. Einzelheiten finden Sie in der SPEKEAPISpezifikation.

Neu bei SPEKE?

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

Eine Einführung in das SPEKE finden Sie im folgenden Webcast:

Verwandte Serviceinformationen und Spezifikationen

- APIGateway-Berechtigungen — So steuern Sie den Zugriff auf eine API mit AWS Identity and Access Management (AWSIAM) -Berechtigungen.
- AWS AssumeRole— So verwenden Sie den AWS Security Token Service (AWSSTS), um Rollenfunktionen zu übernehmen.
- AWSSigv4 — So signieren Sie eine HTTP Anfrage mit Signature Version 4.
- DASHCPIX-IF-Spezifikation v2.0 — Die Spezifikationsversion des DASH -IF Content Protection Information Exchange Format (CPIX), auf der diese Spezifikation SPEKE v1.0 basiert.
- DASHCPIX-IF-Spezifikation v2.3 — Die Spezifikationsversion des DASH -IF Content Protection Information Exchange Format (CPIX), auf der diese v2.0-Spezifikation basiert. SPEKE
- DASH-IF-System IDs — Die Liste der registrierten Identifikatoren für Systeme. DRM
- https://github.com/awslabs/speke-reference-server— Beispiel für einen Referenzschlüsselanbieter, den Sie mit Ihrem AWS Konto verwenden können, um Ihnen den Einstieg in eine SPEKE Implementierung zu erleichtern. AWS

Terminologie

Die folgende Liste definiert die in dieser Spezifikation verwendete Terminologie. Soweit möglich, folgt diese Spezifikation der Terminologie, die in der DASHCPIX-IF-Spezifikation verwendet wurde.

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

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

- DRM— Verwaltung digitaler Rechte. Wird verwendet, um urheberrechtlich geschützte digitale Inhalte vor nicht genehmigtem Zugriff zu schützen.
- DRMPlattform — Ein System, das DRM Funktionen und Unterstützung für Inhaltsverschlüsseler und -betrachter bereitstellt, einschließlich der Bereitstellung von DRM Schlüsseln und Lizenzierung für die Verschlüsselung und Entschlüsselung von Inhalten.
- DRMAnbieter — siehe DRM Plattform.
- DRMSystem — Ein Standard für DRM Implementierungen. Zu den gängigen DRM Systemen gehören Apple FairPlay, Google Widevine und Microsoft. PlayReady DRMSysteme werden von Inhaltsanbietern verwendet, um digitale Inhalte für die Bereitstellung an Zuschauer und für den Zugriff durch Zuschauer zu sichern. Eine Liste der DRM Systeme, die bei DASH -IF registriert sind, finden Sie unter DASH-IF system. IDs Die DASHCPIX-IF-Spezifikation verwendet den Begriff „DRMSystem“, wie er hier definiert ist, und an einigen Stellen verwendet sie den Begriff „DRMSystem“, um das zu bezeichnen, was in dieser Spezifikation als Plattform bezeichnet wird. DRM
- DRMLösung — Siehe DRM Plattform.
- DRMTechnologie — siehe DRM System.
- Encryptor — Eine Medienverarbeitungskomponente, die Medieninhalte mithilfe von Schlüsseln verschlüsselt, die vom Schlüsselanbieter bezogen wurden. Verschlüsseler fügen den Medien in der Regel auch DRM Verschlüsselungssignale und Metadaten hinzu. Verschlüsseler sind in der Regel Encoder, Packager und Transcoder.
- Schlüsselanbieter — Die Komponente einer DRM Plattform, die einen SPEKE REST API zur Bearbeitung von Schlüsselanfragen bereitstellt. Der Schlüsselanbieter kann der Schlüsselserver selbst oder eine andere Komponente der Plattform sein.
- Schlüsselserver — Die Komponente einer DRM Plattform, die Schlüssel für die Verschlüsselung und Entschlüsselung von Inhalten verwaltet.
- Betreiber — Eine Person, die für den Betrieb des Gesamtsystems, einschließlich des Verschlüsselers und des Schlüsselanbieters, verantwortlich ist.
- Player — Ein Mediaplayer, der im Auftrag eines Zuschauers arbeitet. Ruft seine Informationen aus verschiedenen Quellen ab, einschließlich Medienmanifestdateien, Mediendateien und DRM Lizenzen. Fordert im Namen der Zuschauer Lizenzen von der DRM Plattform an.

Kunden-Onboarding für SPEKE

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

Themen

- Beginnen Sie mit einem DRM Plattformanbieter
- SPEKEUnterstützung bei Dienstleistungen und Produkten AWS
- SPEKEUnterstützung bei AWS Partnerdienstleistungen und -produkten

Beginnen Sie mit einem DRM Plattformanbieter

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

DRMPlattformanbieter	SPEKEv1-Unterstützung	SPEKEv2-Unterstützung
Axinom	√	√
Kaufen DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKANetzwerke	√	√

DRMPlattformanbieter	SPEKEv1-Unterstützung	SPEKEv2-Unterstützung
Insys Cloud DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√
JW-Spieler	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKEUnterstützung bei Dienstleistungen und Produkten AWS

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

AWSService oder Produkt	SPEKEv1-Unterstützung	SPEKEv2-Unterstützung	Unterstützte DRM Technologien
AWSElemental MediaConvert — Dienst, der in der AWS Cloud läuft	√	√	Dokumentation

AWSService oder Produkt	SPEKEv1-Unterstützung	SPEKEv2-Unterstützung	Unterstützte DRM Technologien
AWSElemental MediaPackage — Dienst, der in der AWS Cloud läuft	√	√	Dokumentation
AWSElemental Live — Produkt vor Ort	√		Dokumentation: MPEG -/DASHHLS
AWSElemental Server — Lokales Produkt	√		Dokumentation

SPEKEUnterstützung bei AWS Partnerdienstleistungen und -produkten

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

AWSService oder Produkt	SPEKEv1-Unterstützung	SPEKEv2-Unterstützung	Unterstützte DRM Technologien
Bitmovin Live-Videokodierung	√		Dokumentation
Bitmovin Video-on-Demand () Codierung VOD	√		Dokumentation

SPEKEAPISpezifikation

Dies ist die REST API Spezifikation für Secure Packager und Encoder Key Exchange ()SPEKE. Verwenden Sie diese Spezifikation, um Kunden, die Verschlüsselung verwenden, DRM urheberrechtlichen Schutz zu bieten.

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

Diese Spezifikation hat folgende Ziele:

- Definieren Sie eine einfache, vertrauenswürdige und hochsichere Schnittstelle, über die DRM Anbieter und Kunden Verschlüsselungsprogramme integrieren können, wenn Inhaltsverschlüsselung erforderlich ist.
- VODDeckt Workflows ab und bezieht die Fehlerbedingungen und Authentifizierungsmechanismen mit ein, die für eine robuste, hochsichere Kommunikation zwischen Verschlüsselern und den Endpunkten der DRM Schlüsselanbieter erforderlich sind.
- Beinhaltet Unterstützung für HLSMSS, und DASH Paketierung und deren gemeinsame DRM Systeme: FairPlay, PlayReady, und Widevine/. CENC
- Halten Sie die Spezifikation einfach und erweiterbar, um future DRM Systeme zu unterstützen.
- Verwenden Sie eine einfache RESTAPI.

> **Note**
>
>

HOLDERS VON THIS MATERIAL SEIN LIABLE FOR ANYCLAIM, DAMAGES ODER OTHERLIABILITY, WHETHER IN EINEM ACTION VONCONTRACT, TORT ODER OTHERWISE ARISINGFROM, OUT VON ODER IN CONNECTION WITH THIS MATERIAL ODER THE USE ODER OTHER DEALINGS VON THISMATERIAL.

Themen

- Authentifizierung erforderlich für SPEKE
- SPEKEAPIv1
- SPEKEAPIv2
- Lizenz für die Spezifikation SPEKE API

Authentifizierung erforderlich für SPEKE

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

Themen

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

Authentifizierung für AWS Cloud-Implementierungen

SPEKEerfordert eine AWS Authentifizierung über IAM Rollen für die Verwendung mit einem Verschlüsseler. IAMRollen werden vom DRM Anbieter oder vom Betreiber erstellt, dem der DRM Endpunkt in einem AWS Konto gehört. Jeder Rolle wird ein Amazon-Ressourcenname (ARN) zugewiesen, den der AWS Elemental-Servicebetreiber auf der Servicekonsole angibt, wenn er die Verschlüsselung anfordert. Die Richtlinienberechtigungen der Rolle müssen so konfiguriert werden, dass sie die Erlaubnis zum Zugriff auf den Schlüsselanbieter API und keinen anderen AWS Ressourcenzugriff gewähren. Wenn der Verschlüsseler den DRM Schlüsselanbieter kontaktiert, verwendet er die Rolle, ARN um die Rolle des Kontoinhabers des Schlüsselanbieters zu übernehmen. Dieser gibt temporäre Anmeldeinformationen zurück, die der Verschlüsseler für den Zugriff auf den Schlüsselanbieter verwenden kann.

Eine gängige Implementierung besteht darin, dass der Betreiber oder DRM Plattformanbieter Amazon API Gateway vor dem Schlüsselanbieter verwendet und dann die AWS Identity and Access

Management (AWSIAM) -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 eine RolleARN, die für den Zugriff auf den DRM Schlüsselanbieter erstellt wurde:

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

Weitere Informationen zur Erstellung einer Rolle finden Sie unter AWS AssumeRole. Weitere Informationen zum Signieren einer Anfrage finden Sie unter AWSSigv4.

Authentifizierung für lokale Produkte

Für lokale Produkte empfehlen wir die Verwendung vonSSL/TLS- und Digest-Authentifizierung aus Sicherheitsgründen. Sie sollten jedoch mindestens die Standardauthentifizierung über verwenden. HTTPS

Beide Authentifizierungstypen verwenden den `Authorization` Header in der HTTP Anfrage:

- Digest-Authentifizierung — Der Autorisierungsheader besteht aus dem Identifier, `Digest` gefolgt von einer Reihe von Werten, die die Anfrage authentifizieren. Insbesondere wird ein Antwortwert

durch eine Reihe von MD5 Hashfunktionen generiert, zu denen eine eindeutige one-time-use Nonce vom Server gehört, mit der sichergestellt wird, dass das Passwort sicher übertragen wird.

- Standardauthentifizierung — Der Autorisierungsheader besteht aus der Kennung, `Basic` gefolgt von einer Base-64-kodierten Zeichenfolge, die den Benutzernamen und das Passwort darstellt, getrennt durch einen Doppelpunkt.

Informationen zur Standard- und Digest-Authentifizierung, einschließlich detaillierter Informationen zum Header, finden Sie in der Internet Engineering Task Force (IETF) -Spezifikation RFC2617 — HTTP Authentifizierung: Basic and Digest Access Authentication.

SPEKEAPIv1

Dies ist die Version REST API 1 für Secure Packager und Encoder Key Exchange (SPEKE). Verwenden Sie diese Spezifikation, um Kunden, die Verschlüsselung verwenden, DRM urheberrechtlichen Schutz zu bieten. Um SPEKE -konform zu sein, muss Ihr DRM Schlüsselanbieter die in dieser Spezifikation REST API beschriebenen Informationen offenlegen. Der Verschlüsseler API ruft Ihren Schlüsselanbieter an.

> **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.

SPEKEverwendet die Datenstrukturdefinition des DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) für den Schlüsselaustausch, allerdings mit einigen Einschränkungen. DASH-IF- CPIX definiert ein Schema, das einen erweiterbaren DRM Mehrfachaustausch von der DRM Plattform bis zum Verschlüsseler ermöglicht. So wird für alle Verpackungsformate mit adaptiven Bitraten zum Zeitpunkt der Inhaltkompression und -verpackung Inhaltsverschlüsselung bereitgestellt. Zu den Paketformaten mit adaptiver Bitrate gehörenHLS, und. DASH 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

- SPEKEAPIv1 — Anpassungen und Einschränkungen der -IF-Spezifikation DASH

- SPEKEAPIv1 — Standard-Payload-Komponenten
- SPEKEAPIv1 — Beispiele für Live-Workflow-Methodenaufrufe
- SPEKEAPIv1 — Beispiele für VOD Workflow-Methodenaufrufe
- SPEKEAPIv1 — Verschlüsselung von Inhaltsschlüsseln
- SPEKEAPIv1 — Heartbeat
- SPEKEAPIv1 — Überschreiben der Schlüssel-ID

SPEKEAPIv1 — Anpassungen und Einschränkungen der -IF-Spezifikation DASH

Die DASH CPIX -IF-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 Verschlüsseler-Consumer-Workflow.
- Für verschlüsselte Inhaltsschlüssel SPEKE gelten die folgenden Einschränkungen:
  - SPEKEunterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
  - SPEKEerfordert 2048 RSA basierte Zertifikate.
- Für rotierende wichtige Workflows SPEKE ist der `ContentKeyUsageRule` Filter erforderlich,`KeyPeriodFilter`. SPEKEignoriert alle anderen `ContentKeyUsageRule` Einstellungen.
- SPEKE verwendet die `UpdateHistoryItemList`-Funktionalität nicht. Wenn die Liste in der Antwort enthalten ist, wird SPEKE sie ignoriert.
- SPEKEunterstützt die Schlüsselrotation. SPEKEverwendet nur `ContentKeyPeriod@index, um den Schlüsselzeitraum zu verfolgen.
- SPEKEVerwendet zur Unterstützung MSS PlayReady einen benutzerdefinierten Parameter unter dem `DRMSystem` Tag,`SPEKE:ProtectionHeader`.
- Wenn der beim HLS Paketieren in der Antwort vorhanden `URIExtXKey` ist, muss er die vollständigen Daten enthalten, die dem URI `EXT-X-KEY` Tag-Parameter einer HLS Playlist hinzugefügt werden können, ohne dass weitere Signalisierungen erforderlich sind.

- Für HLS Playlisten stehen unter dem `DRMSystem` Tag die optionalen benutzerdefinierten Parameter `speke:KeyFormat` und `speke:KeyFormatVersions` für die Werte des Tags `KEYFORMAT` und die `KEYFORMATVERSIONS` `EXT-X-KEY` Tag-Parameter zur SPEKE Verfügung.

  Der HLS Initialisierungsvektor (IV) folgt immer der Segmentnummer, sofern nicht ausdrücklich vom Operator angegeben.
- 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.
- SPEKEunterstützt derzeit nicht mehrere Tracks oder Keys pro Inhalt.

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

SPEKEAPIv1 — Standard-Payload-Komponenten

Bei jeder SPEKE Anfrage kann der Verschlüsseler Antworten für ein oder mehrere DRM Systeme anfordern. Der Verschlüsseler spezifiziert die DRM Systeme in `<cpix:DRMSystemList>` der Nutzlast der Anfrage. 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`	Eindeutiger Bezeichner für den DRM Systemtyp, wie er bei der DASH IF-Organi sation registriert ist. Eine Liste finden Sie unter DASH-IF System IDs.
`kid`	Die Schlüssel-ID. Dies ist nicht der eigentliche Schlüssel, sondern eine ID, die in einer Hash-Tabelle auf den Schlüssel verweist.
`<cpix:UriExtXKey>`	Fordert einen unverschlüsselten Standards chlüssel an. Der Schlüsselantworttyp muss entweder diese oder die PSSH-Antwort sein.
`<cpix:PSSH>`	Fordert einen schutzsystemspezifischen Header an (PSSH). Dieser Headertyp enthält als Teil von Common Encryption (CENC) einen Verweis auf die, die sowie benutzerdefinierte Daten für den DRM Hersteller. `kid` `systemID` Der Schlüsselantworttyp muss entweder diese oder die `UriExtXKey` -Antwort sein.

_Beispielanfragen für Standardschlüssel und für PSSH _

Das folgende Beispiel zeigt einen Teil einer Beispielanforderung vom Verschlüsseler an den DRM Schlüsselanbieter, wobei die Hauptkomponenten hervorgehoben sind. Die erste Anfrage bezieht sich auf einen Standardschlüssel, während die zweite Anfrage auf eine PSSH Antwort gerichtet ist:

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

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

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

_Beispielantworten für Standard Key und für PSSH _

Das folgende Beispiel zeigt die entsprechende Antwort des DRM Schlüsselanbieters an 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>
```

SPEKEAPIv1 — Beispiele für Live-Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Das Folgende URL ist ein Beispiel und weist nicht auf ein festes Format hin:

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

Anforderungstext

Ein CPIX Element.

Anforderungs-Header

Name	Typ	Auftreten	Beschreibung
`AWS Authorization`	String	1..1	Siehe AWSSigv4

Name	Typ	Auftreten	Beschreibung
`X-Amz-Security-Token`	String	1..1	Siehe Sigv4 AWS
`X-Amz-Date`	String	1..1	Siehe Sigv4 AWS
`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 Payload-Antwort
`4XX (Client error)`	Client-Fehlermeldung	1..1	Beschreibung des Client-Fehlers.
`5XX (Server error)`	Server-Fehlermeldung	1..1	Beschreibung des Server-Fehlers.

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

Beispiel für eine Live-Anforderungsnutzlast mit entschlüsselten Schlüsseln

Das folgende Beispiel zeigt eine typische Payload für Live-Anfragen 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>
```

SPEKEAPIv1 — Beispiele für VOD Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Das Folgende URL ist ein Beispiel und weist nicht auf ein festes Format hin.

```
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- Antwort auf die CPIX Nutzlast
`4XX (Client error)`	Client-Fehlermeldung	1..1	Beschreibung des Client-Fehlers.
`5XX (Server error)`	Server-Fehlermeldung	1..1	Beschreibung des Server-Fehlers.

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

VODBeispiel für eine Payload-Anfrage mit gelöschten Schlüsseln

Das folgende Beispiel zeigt eine grundlegende Payload für VOD Anfragen 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>
```

VODBeispiel für eine Antwort-Payload mit Schlüsseln im Klartext

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>
```

SPEKEAPIv1 — Verschlüsselung von Inhaltsschlüsseln

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

Um die Inhaltsschlüsselverschlüsselung für in der AWS Cloud ausgeführte Verschlüsselungsprogramme zu verwenden, importieren Kunden Zertifikate in den AWS Certificate Manager und verwenden das resultierende Zertifikat dann ARNs für ihre Verschlüsselungsaktivitäten.

Der Verschlüsseler verwendet das Zertifikat ARNs und den ACM Dienst, um dem Schlüsselanbieter verschlüsselte DRM Inhaltsschlüssel zur Verfügung zu stellen.

Einschränkungen

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

- SPEKEunterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
- SPEKEerfordert 2048 RSA basierte Zertifikate.

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

Implementieren der Inhaltsschlüssel-Verschlüsselung

Um die Verschlüsselung von Inhaltsschlüsseln bereitzustellen, schließen Sie Folgendes in Ihre DRM Schlüsselanbieter-Implementierungen ein:

- 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>
```

SPEKEAPIv1 — Heartbeat

Beispiel für eine Anforderungssyntax

Das Folgende URL ist ein Beispiel und weist nicht auf ein festes Format hin:

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

Request Response (Antwort anfordern)

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

SPEKEAPIv1 — Überschreiben der Schlüssel-ID

Der Verschlüsseler erstellt jedes Mal, wenn er Schlüssel wechselt, eine neue Schlüssel-ID (KID). Er leitet den in seinen KID Anfragen an den DRM Schlüsselanbieter weiter. Fast immer antwortet der Schlüsselanbieter mit demselbenKID, aber er kann KID in der Antwort einen anderen Wert für den angeben.

Im Folgenden finden Sie eine Beispielanforderung mit dem 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 den Wert KID von`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>
```

SPEKEAPIv2

Dies ist der REST API für Secure Packager und Encoder Key Exchange (SPEKE) v2. Verwenden Sie diese Spezifikation, um Kunden, die Verschlüsselung verwenden, DRM urheberrechtlichen Schutz zu bieten. Um SPEKE -konform zu sein, muss Ihr DRM Schlüsselanbieter die in dieser Spezifikation REST API beschriebenen Informationen offenlegen. Der Verschlüsseler API ruft Ihren Schlüsselanbieter an.

> **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.

SPEKEverwendet die Datenstrukturdefinition des DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) für den Schlüsselaustausch, allerdings mit einigen Einschränkungen. DASH-IF- CPIX definiert ein Schema, das einen erweiterbaren DRM Mehrfachaustausch von der DRM Plattform bis zum Verschlüsseler ermöglicht. So wird für alle Verpackungsformate mit adaptiven Bitraten zum Zeitpunkt der Inhaltkompression und -verpackung Inhaltsverschlüsselung bereitgestellt. Zu den Paketformaten mit adaptiver Bitrate gehörenHLS, und. DASH MSS

Beginnend mit der Version 2.0 SPEKE ist es auf eine bestimmte CPIX Version ausgerichtet:

Auf der einen SPEKE Seite wird dies durch die Verwendung des `X-Speke-Version` HTTP Headers und auf der CPIX anderen Seite durch die Verwendung des `CPIX@version` Attributs erzwungen. Das Fehlen dieser Elemente in den Anfragen ist typisch für ältere SPEKE V1-Workflows. In SPEKE v2-Workflows wird erwartet, dass der Schlüsselanbieter CPIX Dokumente nur verarbeitet, wenn er beide Versionsparameter unterstützt.

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

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

- Alle Tags aus dem SPEKE XML Namespace sind veraltet und werden durch äquivalente Tags im Namespace ersetzt CPIX XML
- `SPEKE:ProtectionHeader`ist veraltet und wird ersetzt durch `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`, `SPEKE:KeyFormat` und `SPEKE:KeyFormatVersions` sind veraltet und wurden ersetzt durch `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id`wird ersetzt durch `CPIX@contentId`
- Neue obligatorische CPIX Attribute:`CPIX@version`, `ContentKey@commonEncryptionScheme`
- Neues optionales CPIX Element: `DRMSystem.ContentProtectionData`
- Support für mehrere Inhaltsschlüssel
- Versionsübergreifender Mechanismus zwischen und SPEKE CPIX
- HTTPEntwicklung der Header: neuer `X-Speke-Version` Header, Header umbenannt in `Speke-User-Agent` `X-Speke-User-Agent`
- Heartbeat API ist veraltet

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

Themen

- SPEKEAPIv2 — Anpassungen und Einschränkungen der -IF-Spezifikation DASH
- SPEKEAPIv2 — Standard-Payload-Komponenten
- SPEKEAPIv2 - Verschlüsselungsvertrag
- SPEKEAPIv2 — Beispiele für Live-Workflow-Methodenaufrufe
- SPEKEAPIv2 — Beispiele für VOD Workflow-Methodenaufrufe
- SPEKEAPIv2 — Verschlüsselung von Inhaltsschlüsseln
- SPEKEAPIv2 — Überschreiben der Schlüssel-ID

SPEKEAPIv2 — Anpassungen und Einschränkungen der -IF-Spezifikation DASH

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

CPIXProfil

- SPEKE folgt dem Verschlüsseler-Consumer-Workflow.
- Für verschlüsselte Inhaltsschlüssel SPEKE gelten die folgenden Einschränkungen:
  - SPEKEunterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
  - SPEKEerfordert 2048 RSA basierte Zertifikate.
- SPEKEnutzt nur einen Teil der Funktionen: CPIX
  - SPEKE verwendet die `UpdateHistoryItemList`-Funktionalität nicht. Wenn die Liste in der Antwort enthalten ist, wird SPEKE sie ignoriert.
  - SPEKElässt die Root-/Leaf-Tasten-Funktionalität aus. Wenn das `ContentKey@dependsOnKey` Attribut in der Antwort vorhanden ist, wird es ignoriert. SPEKE
  - SPEKElässt das `BitrateFilter` Element und das `VideoFilter@wcg` Attribut aus. Wenn diese Elemente oder Attribute in der CPIX Nutzlast vorhanden sind, wird SPEKE sie ignoriert.

- In CPIX Dokumenten, die mit Version 2 ausgetauscht werden, können nur die Elemente oder Attribute verwendet werden, auf die auf der Seite „Standard-Payload-Komponenten“ oder auf der Seite „Verschlüsselungsvertrag“ als „Unterstützt“ verwiesen wird. SPEKE
- Wenn sie in einer CPIX Anfrage des Verschlüsselers enthalten sind, müssen alle Elemente und Attribute in der Antwort des Schlüsselanbieters CPIX einen gültigen Wert enthalten. Wenn nicht, stoppt der Verschlüsseler und gibt einen Fehler aus.
- SPEKEunterstützt die Schlüsselrotation mit `KeyPeriodFilter` Elementen. SPEKEverwendet nur die`ContentKeyPeriod@index`, um den Schlüsselzeitraum zu verfolgen.
- Für die HLS Signalisierung müssen mehrere `DRMSystem.HLSSignalingData` Elemente verwendet werden: eines mit dem `DRMSystem.HLSSignalingData@playlist` Attributwert „media“ und eines mit dem `DRMSystem.HLSSignalingData@playlist` Attributwert „master“.
- Beim Anfordern von Schlüsseln verwendet der Verschlüsseler möglicherweise das optionale Attribut `@explicitIV` des Elements `ContentKey`. Der Schlüsselanbieter kann mit einem IV unter Verwendung von `@explicitIV` antworten, auch wenn das Attribut nicht in der Anforderung enthalten ist.
- Die Verschlüsseler erstellt die Schlüssel-ID (`KID`), die für alle Inhalts-IDs und Schlüsselzeiträume gleich bleibt. Der Schlüsselanbieter schließt `KID` in seiner Antwort auf das Anforderungsdokument ein.
- Der Verschlüsseler muss einen Wert für das Attribut enthalten. `CPIX@contentId` Wenn der Schlüsselanbieter einen leeren Wert für dieses Attribut erhält, gibt er einen Fehler mit der Beschreibung „Missing CPIX @contentId“ zurück. `CPIX@contentId`Der Wert kann vom Schlüsselanbieter nicht überschrieben werden.

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

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

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

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

`ContentKey@commonEncryptionScheme`Der Wert kann vom Schlüsselanbieter nicht überschrieben werden.

- Beim Empfang verschiedener Werte für `DRMSystem@PSSH` XML `<pssh>` ein `DRMSystem.ContentProtectionData` inneres Element im CPIX Antworttext stoppt der Verschlüsseler und gibt einen Fehler aus.

API für CPIX

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

  Der vom Verschlüsseler definierte `X-Speke-Version` Header-Wert kann vom Schlüsselanbieter in der Antwort auf die Anfrage nicht geändert werden.
- Beim Empfang von Fehlern im Antworttext gibt der Verschlüsseler einen Fehler aus und versucht die Anfrage nicht erneut mit einer SPEKE Version 1.0.

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

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

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

Fehlerfall	Fehlermeldung
Der Verschlüsselungsvertrag enthält keine VideoFilter AudioFilter OR-Elemente	Fehlender CPIX Verschlüsselungsvertrag

SPEKEAPIv2 — Standard-Payload-Komponenten

Mit einer einzigen SPEKE Anfrage kann der Verschlüsseler mehrere Inhaltsschlüssel zusammen mit der erforderlichen Manifestsignalisierung für mehrere Verpackungsformate anfordern, je nach dem Verschlüsselungsvertrag, der für einen bestimmten Inhalt definiert ist.

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

<cpix: ContentKeyList > Abschnitt und oberste Ebene <cpix : >Element CPIX

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

Gemäß der CPIX Spezifikation sind die möglichen Werte des `ContentKey@commonEncryptionScheme` Attributs in der Spezifikation Common Encryption in ISO Base Media File Format (ISO/IEC23001-7:2016) definiert:

- 'cenc': CTR Modus zur Verschlüsselung von Vollproben und AES Video-Subsamples NAL
- 'cbc1': AES - CBC Modus zur Verschlüsselung von vollständigen Samples und Video-Subsamples NAL
- 'cens': AES Modus zur teilweisen Verschlüsselung von Videomustern CTR NAL
- 'cbcs': CBC Modus zur teilweisen Verschlüsselung von AES Videomustern NAL

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

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

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

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

Element unterstützt von SPEKE	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : >CPIX	contentId , Version, xmlns:cpix, xmlns:pskc	name, xmlns:enc	eins <cpix: ContentKeyList >, eins<cpix : >, eins <cpix : >DRMSyste mListCont entKeyUsa geRuleList	ein<cpix : >, eins <cpix : >Delivery DataListC ontentKey PeriodList
<cpixCont entKeyList: >	-	id	mindesten s ein <cpix : >ContentKey	-
<cpix : >ContentKey	Kind, Data commonEnc ryptionScheme	id, Algorithmus, explizite IV	eins <pskc:Sec ret>	-

Element unterstützt von SPEKE	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<pskc:Secret>	PlainValue oder EncryptedValue	Wert MAC	-	<enc: EncryptionMethod >, <enc : >CipherData

<cpix : >Abschnitt DRMSystemList

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

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

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

Eine vollständige Liste von DRM systemIDs finden Sie im Abschnitt Inhaltsschutz des Repositorys DASH -IF Identifiers.

Element unterstützt von SPEKE	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : >DRMSystemList	-	id	mindestens ein <cpix : >DRMSystem	-
<cpix : >DRMSystem	Kind, systemId	ID, Name, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHeaderData, zwei <cpix: HLSSignalingData > - Elemente mit unterschiedlichen Playlist-Attributwerten

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

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

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

<cpix : >Abschnitt ContentKeyPeriodList

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

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

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

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

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

<cpix : >Abschnitt ContentKeyUsageRuleList

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

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

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

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

Element unterstützt von SPEKE	Obligatorische Attribute	Optionale Attribute	Obligatorische untergeordnete Elemente	Optionale untergeordnete Elemente
<cpix : >ContentKeyUsageRuleList	-	id	mindestens ein <cpix : >ContentKeyUsageRule	-
<cpix : >ContentKeyUsageRule	Kind, intendedTrackType	-	mindestens ein <cpix: AudioFilter > oder ein <cpix : >(*) VideoFilter	<cpix : >KeyPeriodFilter
<cpix : >KeyPeriodFilter	periodId	-	-	-
<cpix : >AudioFilter	-	minChannels, maxChannels	-	-
<cpix : >VideoFilter	-	minPixels,, hdrmaxPixels, minFps maxFps	-	-

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

SPEKEAPIv2 - Verschlüsselungsvertrag

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

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

Prinzipien

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

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

Für diese Beziehung gelten folgende Regeln:

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

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

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

Filter

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

CPIXFiltertyp	Allgemeine SPEKE Unterstützung	Filterattribute werden unterstützt von SPEKE	Filterattribute werden nicht unterstützt von SPEKE
<cpix : >VideoFilter	Ja	minPixels, hdrmaxPixels,minFps, maxFps (optionale Attribute)	wcg
<cpix : >AudioFilter	Ja	minChannels, maxChannels (optionale Attribute)	
<cpix : >KeyPeriodFilter	Ja	periodId (obligatorisches Attribut)	
<cpix : >BitrateFilter	Nein	N/A	N/A

CPIXFiltertyp	Allgemeine SPEKE Unterstützung	Filterattribute werden unterstützt von SPEKE	Filterattribute werden nicht unterstützt von SPEKE
<cpix : >LabelFilter	Nein	N/A	N/A

Gemäß der CPIX Spezifikation für ist [VideoFilterminPixels,maxPixels] ein All-Inclusive-Bereich in beiden Dimensionen, während (minFps,maxFps] nur für die Dimension inklusiv ist. maxFps Denn [AudioFilterminChannels,maxChannels] ist ein inklusiver Bereich in beiden Dimensionen.

Problematische Situationen

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

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

In dieser Situation	Der Verschlüsseler sollte/soll...	Der Schlüsselanbieter sollte/ soll...
um einen bestimmten Titel zu verschlüsseln	Code in der Reihenfolge des Dokuments anwenden.	
Der Verschlüsselungsvertrag ändert sich in einem einzigen SPEKE Anforderungs-/Antwortzyklus	Der Verschlüsseler löst eine Ausnahme aus und stoppt die Verarbeitung, da der Schlüsselanbieter nicht für die Definition des Verschlüsselungsvertrags verantwortlich ist.	Um zu verhindern, dass diese Situation von vornherein eintritt, darf der Schlüsselanbieter einen Verschlüsselungsvertrag, den er in der CPIX Payload der SPEKE Anfrage erhalten hat, nicht ändern.
Fehlerhafter Verschlüsselungsvertrag: Ausnahme bei der Kardinalitätsbeschränkung intendedTrackType /Filters, nicht unterstützte Filter oder Attribute	Der Verschlüsseler muss eine Ausnahme auslösen, die Verarbeitung beenden und die SPEKE Anfrage nicht an den Schlüsselanbieter senden, da dies höchstwahrscheinlich zu einem fehlerhaften Schutz der Inhalte führen oder einige Spuren ungeschützt lassen würde.	Der Schlüsselanbieter löst eine Ausnahme aus und gibt die Fehlermeldung „Fehlerhafter Verschlüsselungsvertrag“ zurück.
Gut formulierter Verschlüsselungsvertrag, der jedoch gegen die Einschränkungen der DRM Sicherheitsstufen verstößt: Beispielsweise wird ein einziger Inhaltsschlüssel angefordert, um sowohl Audio- als auch Videospuren zu schützen UHD	Wenn der Verschlüsseler die Einschränkungen der DRM Sicherheitsstufen kennt, sollte er eine Ausnahme auslösen, die Verarbeitung beenden und die SPEKE Anfrage nicht an den Schlüsselanbieter senden, da dies höchstwahrscheinlich zu einem fehlerhaften Schutz der Inhalte führen würde.	Der Schlüsselanbieter löst eine Ausnahme aus und gibt die Fehlermeldung „Angeforderter CPIX Verschlüsselungsvertrag wird nicht unterstützt“ zurück.

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

Beispiele für Verschlüsselungsverträge

Beispiel 1: Ein Inhaltsschlüssel für alle Audio- und Videotracks

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

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

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

Beispiel 3: ein Inhaltsschlüssel für alle Videospuren, unverschlüsselte Audiospuren

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

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

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

Beispiel 5: mehrere Inhaltstasten 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 Inhaltstasten 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 Inhaltstasten für verschiedene Videospuren (SD///HD1HD2UHD1/UHD2), ein Inhaltsschlüssel für alle Audiospuren

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

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

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

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

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

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

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

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

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

SPEKEAPIv2 — Beispiele für Live-Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Das Folgende URL ist ein Beispiel und weist nicht auf ein festes Format hin:

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

Anforderungstext

Ein CPIX Dokument.

Anforderungs-Header

Name	Typ	Auftreten	Beschreibung
`AWS Authorization`	String	1..1	Siehe AWSSigv4
`X-Amz-Security-Token`	String	1..1	Siehe Sigv4 AWS
`X-Amz-Date`	String	1..1	Siehe Sigv4 AWS
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	SPEKEAPIVersion, die mit der Anfrage verwendet wurde, formuliert als MajorVersion.

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

Antwort-Header

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

Request Response (Antwort anfordern)

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

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

Beispiel für eine Live-Anforderungsnutzlast mit entschlüsselten Schlüsseln

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

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

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

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

Beispiel für eine Live-Antwortnutzlast mit entschlüsselten Schlüsseln

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

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

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

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

SPEKEAPIv2 — Beispiele für VOD Workflow-Methodenaufrufe

Beispiel für eine Anforderungssyntax

Das Folgende URL ist ein Beispiel und weist nicht auf ein festes Format hin.

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

Anforderungstext

Ein CPIX Dokument.

Anforderungs-Header

Name	Typ	Auftreten	Beschreibung
`AWS Authorization`	String	1..1	Siehe AWSSigv4
`X-Amz-Security-Token`	String	1..1	Siehe Sigv4 AWS
`X-Amz-Date`	String	1..1	Siehe Sigv4 AWS
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	SPEKEAPIV ersion, die mit der Anfrage verwendet wurde, formuliert als MajorVersion. MinorVersion, wie '2.0' für SPEKE v2.0

Antwort-Header

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

Request Response (Antwort anfordern)

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

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

VODBeispiel für eine Payload-Anfrage mit gelöschten Schlüsseln

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

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

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

VODBeispiel für eine Payload für eine Antwort mit unverschlüsselten Schlüsseln

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

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

```
      <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
     </pskc:Secret>
    </cpix:Data>
   </cpix:ContentKey>
   <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
    <cpix:Data>
     <pskc:Secret>
      <pskc:PlainValue>h3toSFIlyAYpfXVQ795m6x==</pskc:PlainValue>
     </pskc:Secret>
    </cpix:Data>
   </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
   <!-- FairPlay -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
    <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
    <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
   </cpix:DRMSystem>
   <!-- Widevine -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
   </cpix:DRMSystem>
   <!-- Playready -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
```

```
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix: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>
```

SPEKEAPIv2 — Verschlüsselung von Inhaltsschlüsseln

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

Um die Inhaltsschlüsselverschlüsselung für in der AWS Cloud ausgeführte Verschlüsselungsprogramme zu verwenden, importieren Kunden Zertifikate in den AWS Certificate Manager und verwenden das resultierende Zertifikat dann ARNs für ihre Verschlüsselungsaktivitäten. Der Verschlüsseler verwendet das Zertifikat ARNs und den ACM Dienst, um dem Schlüsselanbieter verschlüsselte DRM Inhaltsschlüssel zur Verfügung zu stellen.

Einschränkungen

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

- SPEKEunterstützt keine Überprüfung digitaler Signaturen (XMLDSIG) für Payloads von Anfragen oder Antworten.
- SPEKEerfordert 2048 RSA basierte Zertifikate.

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

Implementieren der Inhaltsschlüssel-Verschlüsselung

Um die Verschlüsselung von Inhaltsschlüsseln bereitzustellen, schließen Sie Folgendes in Ihre DRM Schlüsselanbieter-Implementierungen ein:

- 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>
```

SPEKEAPIv2 — Überschreiben der Schlüssel-ID

Der Verschlüsseler erstellt jedes Mal, wenn er Schlüssel wechselt, eine neue Schlüssel-ID (KID). Er leitet den in seinen KID Anfragen an den DRM Schlüsselanbieter weiter. Fast immer antwortet der Schlüsselanbieter mit demselbenKID, aber er kann KID in der Antwort einen anderen Wert für den angeben.

Im Folgenden finden Sie eine Beispielanforderung mit dem 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 den Wert KID von`22222222-2222-2222-2222-222222222222`:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
 kid="22222222-2222-2222-2222-222222222222" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- Widevine -->
  <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
   <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
```

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

Lizenz für die Spezifikation SPEKE API

Creative Commons Namensnennung — ShareAlike 4.0 Internationale öffentliche Lizenz

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

Abschnitt 1: Definitionen.

a. Adaptiertes Material bezeichnet Material, das dem Urheberrecht und vergleichbaren Schutzrechten unterliegt, das aus dem lizenzierten Material abgeleitet ist oder darauf basiert und in dem das lizenzierte Material übersetzt, geändert, angeordnet, transformiert oder anderweitig auf eine Weise modifiziert wurde, die nach Urheberrecht oder vergleichbaren Schutzrechten, die vom Lizenzgeber gehalten werden, eine Erlaubnis erforderlich machen. Im Rahmen dieser öffentlichen Lizenz, bei der das lizenzierte Material ein musikalisches Werk, eine Aufführung oder eine Audioaufnahme ist, entsteht immer adaptiertes Material, wenn das lizenzierte Material zeitlich mit bewegten Bildern synchronisiert wird.
b. Die Lizenz von Adapter bedeutet die Lizenz, die Sie gemäß den Bedingungen dieser Public License auf Ihr Urheberrecht und ähnliche Rechte an Ihren Beiträgen zu adaptiertem Material anwenden.
c. BY-SA-kompatible Lizenz bedeutet eine auf creativecommons.org/compatiblelicenses aufgeführte Lizenz, die von Creative Commons als im Wesentlichen dieser Public License gleichwertig genehmigt wurde.

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

e. Wirksame technische Maßnahmen sind solche Maßnahmen, die ohne entsprechende Befugnisse nicht durch Gesetze zur Erfüllung von Verpflichtungen gemäß Artikel 11 des am 20. Dezember 1996 verabschiedeten WIPO Urheberrechtsvertrags und/oder ähnlichen internationalen Abkommen umgangen werden dürfen.

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

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

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

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

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

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

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

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

Abschnitt 2: Geltungsbereich.

a. Lizenzgewährung.

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

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

   B. adaptiertes Material produzieren, reproduzieren und teilen.

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

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

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

5. Nachfolgende Empfänger.

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

   B. Zusätzliches Angebot des Lizenzgebers — Adaptiertes Material. Jeder Empfänger von adaptiertem Material von Ihnen erhält automatisch ein Angebot des Lizenzgebers, die lizenzierten Rechte an dem adaptierten Material gemäß den Bedingungen der von Ihnen geltenden Adapterlizenz auszuüben.

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

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

b. Andere Rechte.

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

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

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

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

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

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

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

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

2. Sie können die Bedingungen in Abschnitt 3(a)(1) auf beliebige sinnvolle Weise nach Maßgabe von Medium, Mittel und Kontext erfüllen, mit und in dem Sie das lizenzierte Material weitergeben. Beispielsweise kann es sinnvoll sein, die Bedingungen zu erfüllen, indem Sie einen Link URI oder einen Hyperlink zu einer Ressource bereitstellen, die die erforderlichen Informationen enthält.
3. Wenn der Lizenzgeber dies fordert, müssen Sie die gemäß Abschnitt 3(a)(1)(A) erforderlichen Informationen entfernen, soweit dies praktikabel ist.

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

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

Abschnitt 4: Datenbankherstellerrechte.

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

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

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

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

Abschnitt 5: Gewährleistungsausschluss und Haftungsbeschränkung.

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

b. Im größtmöglichen Umfang wird die Haftung des Lizenzgebers Ihnen gegenüber aus beliebigem Rechtsgrund (einschließlich Fahrlässigkeit, ohne darauf beschränkt zu sein) für unmittelbare, konkrete oder mittelbare Schäden, Nebenkosten, Folgeschäden, Strafzahlungen oder Schadenersatz mit Strafcharakter oder andere Verluste, Kosten, Ausgaben oder Schäden, die sich aus dieser öffentlichen Lizenz oder der Nutzung des lizenzierten Materials ergeben, ausgeschlossen, auch wenn der Lizenzgeber über die Möglichkeit solcher Verluste, Kosten, Ausgaben oder Schäden informiert war. Da eine vollständige oder teilweise Haftungsbeschränkung nicht überall zulässig ist, betrifft diese Beschränkung Sie möglicherweise nicht.

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

Abschnitt 6: Laufzeit und Beendigung.

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

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

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

   2. nach ausdrücklicher Wiedereinstellung durch den Lizenzgeber.

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

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

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

Abschnitt 7: Andere Bestimmungen.

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

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

Abschnitt 8: Interpretation.

a. Zur Klarstellung: Diese öffentliche Lizenz stellt keine Einschränkung, Limitierung oder Beschränkung einer Nutzung des lizenzierten Materials dar, unterwirft diese Nutzung keinen

Bedingungen und darf nicht interpretiert werden, als wäre dies ihr Zweck, sofern die betreffende Nutzung rechtmäßig ohne Erlaubnis durch diese öffentliche Lizenz möglich wäre.

b. In dem Umfang, in dem eine Bestimmung dieser öffentlichen Lizenz als undurchsetzbar gefunden wird, wird sie automatisch in geringstmöglichem Umfang umgeformt, um ihre Durchsetzbarkeit zu ermöglichen. Kann die Bestimmung nicht umgeformt werden, ist sie von dieser öffentlichen Lizenz abzutrennen, ohne dass dies die Durchsetzbarkeit der übrigen Bestimmungen beeinträchtigen würde.

c. Ein Rechtsverzicht auf eine der Bestimmungen dieser öffentlichen Lizenz sowie eine Zustimmung zu einem Verstoß gegen die Bestimmungen dieser öffentlichen Lizenz ist nur durch ausdrückliche Vereinbarung seitens des Lizenzgebers möglich.

d. Keine der Aussagen in dieser öffentlichen Lizenz begründet oder darf interpretiert werden als eine Beschränkung der oder ein Verzicht auf Rechte und Privilegien, die für den Lizenzgeber oder Sie gelten, einschließlich der aus rechtlichen Verfahren von Jurisdiktionen oder Behörden erwachsenden Rechte und Privilegien.

Dokumentenhistorie für den SPEKE Partner- und Kundenleitfaden

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

SPEKE v1

Änderung	Beschreibung	Datum
Support-Matrix: Dienstlei stungen und Produkte von AWS Partnern	Es wurde ein neuer Abschnitt für SPEKE Support in AWS Partnerdiensten und -produkte n hinzugefügt, in dem die Bitmovin-Dienste aufgelistet sind.	13. Januar 2023
Updates für DRM Plattform anbieter	Links und neue Partnerin formationen zur Liste der DRM Plattformanbieter hinzugefügt.	24. Januar 2019
Drittanbieter-Verschlüsseler einschließen	Architektur und Beschreib ungen wurden aktualisiert, um Drittanbieter-Verschlüsseler zu berücksichtigen.	20. November 2018
Inhaltsschlüssel-Verschlüss elung	Hinzufügung der Option für die Verschlüsselung von Inhaltssc hlüsseln. Zuvor unterstüt zten Secure Packager und Encoder Key Exchange nur die Bereitstellung von Clear-Keys.	30. Oktober 2018
Unterstützungsmatrix - AWS Elemental Live	Eine AWS Elemental Live-Unterstützungsmatrix wurde hinzugefügt.	27. September 2018

Änderung	Beschreibung	Datum
Nutzlast-Standardkomponente n	Es wurde ein Abschnitt hinzugefügt, der die Hauptelemente in der JSON Payload definiert.	27. September 2018
KIDüberschreiben	Es wurde ein Abschnitt über KID Überschreibungen durch einen Schlüsselanbieter hinzugefügt.	27. September 2018
Die Links zur DASH -IF-Seite wurden korrigiert	Die Links zur DASH IF-Seite für die CPIX Spezifikation und die IDs Systemseite wurden korrigiert.	27. September 2018
Kopie für AWS Elemental Live veröffentlichen	Die SPEKE Dokumentation wurde um AWS Elemental-Produkte aktualisiert.	20. Juli 2018
CMAF	Die Tabellen mit der Unterstüt zungsmatrix für Dienste wurden aktualisiert und enthalten nun das Common Media Application Format (CMAF).	27. Juni 2018

Änderung	Beschreibung	Datum
Erstversion	Erste Version von Secure Packager und Encoder Key Exchange (SPEKE) Version 1, einer Spezifikation für die Kommunikation zwischen einem Inhaltsverschlüsseler und einem DRM Schlüsselanbieter. Der DRM Schlüsselanbieter stellt Secure Packager und Encoder Key Exchange API bereit, um eingehende Schlüsselanfragen zu bearbeiten.	27. November 2017

SPEKE v2

Änderung	Beschreibung	Datum
Aktualisierungen im Bereich DRM Plattformanbieter und im Abschnitt zur Unterstützung von AWS Diensten und Produkten SPEKE	Webstream wurde der SPEKE v2-Spalte der DRM Plattformanbieter-Liste MediaConvert hinzugefügt und der SPEKE v2-Spalte der Tabelle SPEKE Support in AWS Diensten und Produkten hinzugefügt.	10. Oktober 2024
Aktualisierungen im Bereich DRM Plattformanbieter	Der Spalte SPEKE v2 der Liste der DRM Plattformanbieter wurden neue qualifizierte Partner hinzugefügt.	9. August 2023
Aktualisierungen der Abschnitte mit Beispielen für Live- und VOD Workflow-Methodenaufrufe	Fehlender X-Speke-Version Antwort-Header in den Abschnitten SPEKE v2 Live und Beispiele für VOD	13. Januar 2023

Änderung	Beschreibung	Datum
	Workflow-Methodenaufrufe hinzugefügt.	
Aktualisierungen im Bereich DRM Plattformanbieter und Verschlüsselungsverträge	Neue qualifizierte Partner wurden zur Spalte SPEKE v2 der Liste der DRM Plattform anbieter hinzugefügt. Zwei neue Beispiele für Verschlüs selungsverträge wurden hinzugefügt und die maximale SD-Auflösung in allen betroffenen Beispielen auf 1024x576 geändert.	27. Januar 2022
Erstversion	Erste Version von Secure Packager und Encoder Key Exchange (SPEKE), Version 2.0, einer Spezifikation für die Kommunikation zwischen einem Inhaltsverschlüsse ler und einem Schlüssel anbieter. DRM Der DRM Schlüsselanbieter stellt Secure Packager und Encoder Key Exchange API bereit, um eingehende Schlüssel anfragen zu bearbeiten.	7. September 2021

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