Guida per partner e clienti

Specifica API Elemental Secure Packager and Encoder Key Exchange

Specifica API Elemental Secure Packager and Encoder Key Exchange: Guida per partner e clienti

Table of Contents

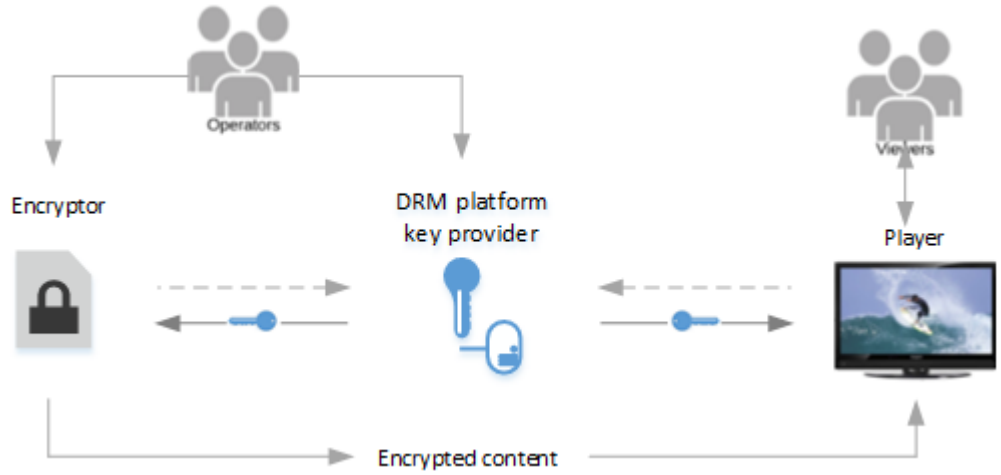
Cos'è Secure Packager and Encoder Key Exchange?

Secure Packager and Encoder Key Exchange (SPEKE) definisce lo standard per la comunicazione tra crittografatori e confezionatori di contenuti multimediali e fornitori di chiavi per la gestione dei diritti digitali (DRM). La specifica è adatta ai componenti di crittografia in esecuzione in locale e nel cloud AWS.

Argomenti

Architettura generale

L'illustrazione seguente mostra una visione di alto livello dell'architettura di crittografia dei contenuti SPEKE per i prodotti locali.



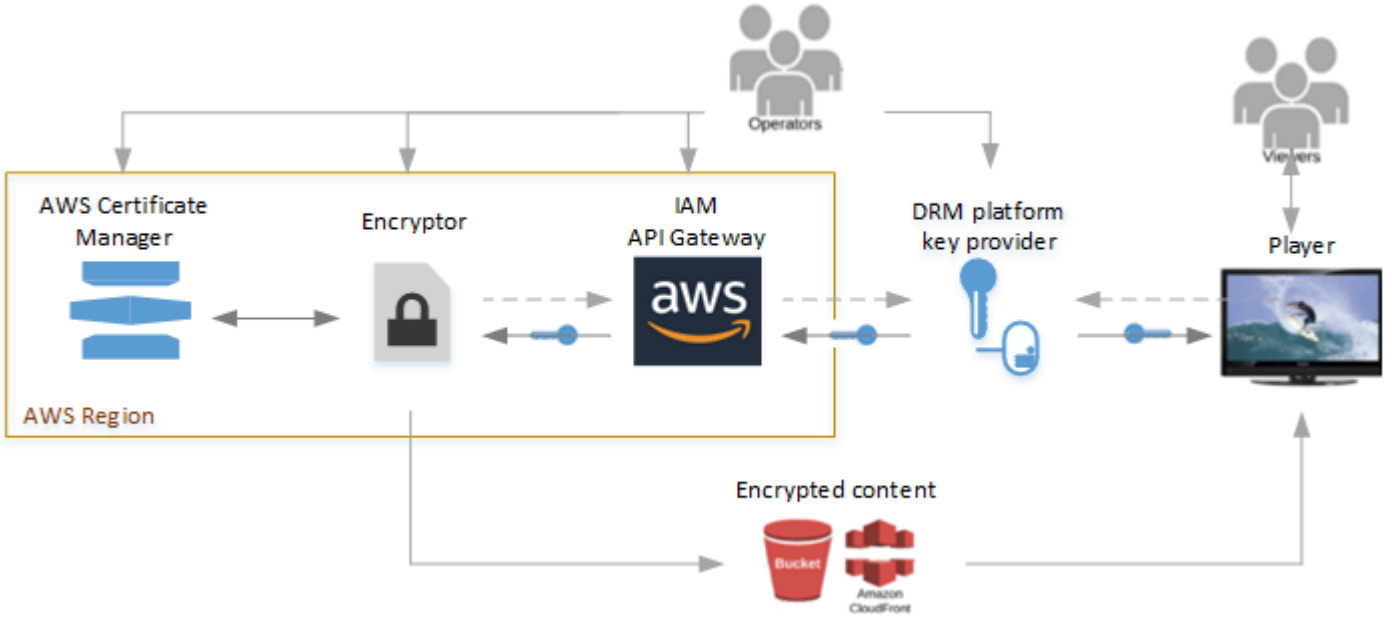
Questi sono i componenti principali dell'architettura precedente:

- Encryptor: fornisce la tecnologia di crittografia. Riceve le richieste di crittografia dall'operatore e recupera le chiavi richieste dal provider di chiavi DRM per proteggere i contenuti crittografati.
- Fornitore di chiavi della piattaforma DRM: fornisce le chiavi di crittografia al crittografo tramite un'API conforme a SPEKE. Il provider fornisce anche le licenze per i lettori multimediali per la decrittografia.

- Player: richiede le chiavi allo stesso fornitore di chiavi della piattaforma DRM, che il giocatore utilizza per sbloccare il contenuto e offrirlo ai suoi spettatori.

Architettura AWS basata sul cloud

La figura seguente mostra l'architettura di alto livello quando SPEKE viene utilizzato con i servizi e le caratteristiche in esecuzione nel cloud AWS.



Questi sono i principali servizi e componenti:

- Encryptor: fornisce la tecnologia di crittografia nel cloud AWS. Il componente di crittografia riceve le richieste dall'operatore e recupera le chiavi di crittografia richieste dal provider di chiavi DRM, tramite Amazon API Gateway, per proteggere i contenuti crittografati. Fornisce i contenuti crittografati a un bucket Amazon S3 o tramite una distribuzione Amazon. CloudFront
- AWS IAM e Amazon API Gateway: gestisce i ruoli affidabili dei clienti e le comunicazioni proxy tra l'encryptor e il provider di chiavi. API Gateway fornisce funzionalità di registrazione e consente ai clienti di controllare le loro relazioni con il componente di crittografia e con la piattaforma DRM. I clienti abilitano l'accesso al provider di chiavi attraverso la configurazione del ruolo IAM. L'API Gateway deve risiedere nella stessa regione AWS del componente di crittografia.
- AWS Certificate Manager — (opzionale) Fornisce la gestione dei certificati per la crittografia delle chiavi di contenuto. La crittografia delle chiavi dei contenuti è la prassi raccomandata per le comunicazioni protette. Il gestore di certificati deve risiedere nella stessa regione AWS del componente di crittografia.

- Provider di chiavi della piattaforma DRM: fornisce chiavi di crittografia al crittografo tramite un'API conforme a SPEKE. Il provider fornisce anche le licenze per i lettori multimediali per la decrittografia.
- Player: richiede le chiavi allo stesso fornitore di chiavi della piattaforma DRM, che il giocatore utilizza per sbloccare il contenuto e offrirlo ai suoi spettatori.

Come iniziare

Per materiale introduttivo aggiuntivo su SPEKE, vedi Sei nuovo su SPEKE? .

Sei un cliente?

Sigla una partnership con un provider della piattaforma DRM AWS Elemental per iniziare a utilizzare la crittografia. Per i dettagli, consulta Customer Onboarding.

Sei un provider della piattaforma DRM o un cliente con un tuo provider di chiavi?

Esponi un'API REST per il tuo fornitore principale in conformità con le specifiche SPEKE. Per i dettagli, consulta le specifiche dell'API SPEKE.

Sei nuovo su SPEKE?

Questa sezione fornisce materiale introduttivo per i lettori che non conoscono Secure Packager e Encoder Key Exchange (SPEKE).

Per un'introduzione a SPEKE, guardate il seguente webcast:

Servizi e specifiche correlati

- Autorizzazioni API gateway: come controllare l'accesso a un'API con le autorizzazioni AWS Identity and Access Management (AWS IAM).
- AWS AssumeRole — Come utilizzare AWS Security Token Service (AWS STS) per assumere la funzionalità del ruolo.
- AWS Sigv4 — Come firmare una richiesta HTTP utilizzando Signature Version 4.
- Specificazione DASH-IF CPIX v2.0 — La versione della specifica DASH-IF Content Protection Information Exchange Format (CPIX), su cui si basa questa specifica SPEKE v1.0.
- Specificazione DASH-IF CPIX v2.3 — La versione della specifica DASH-IF Content Protection Information Exchange Format (CPIX), su cui si basa questa specifica SPEKE v2.0.
- ID di sistema DASH-IF: l'elenco degli identificatori registrati per i sistemi DRM.
- https://github.com/awslabs/ speke-reference-server — Esempio di fornitore di chiavi di riferimento da utilizzare con il tuo account AWS, per aiutarti a iniziare con un'implementazione SPEKE in AWS.

Terminologia

L'elenco seguente definisce la terminologia utilizzata in questa specifica. Laddove possibile, questa specifica segue la terminologia utilizzata nella specifica DASH-IF CPIX.

- ARN: nome della risorsa Amazon. Identifica in modo univoco una risorsa AWS.
- Chiave di contenuto: una chiave crittografica utilizzata per crittografare parte del contenuto.
- Fornitore di contenuti: un editore che fornisce i diritti e le regole per la distribuzione di contenuti multimediali protetti. Il provider di contenuti potrebbe fornire anche i file multimediali sorgente (formato mezzanine, per la transcodifica), gli identificatori degli asset, gli identificatori delle chiavi (KID), i valori delle chiavi, le istruzioni di codifica e i metadati di descrizione dei contenuti.

- DRM: gestione dei diritti digitali. Utilizzato per proteggere i contenuti digitali protetti da copyright da accessi non autorizzati.
- Piattaforma DRM: un sistema che fornisce funzionalità e supporto DRM a crittografatori e visualizzatori di contenuti, inclusa la fornitura di chiavi DRM e licenze per la crittografia e la decrittografia dei contenuti.
- Provider DRM: vedi piattaforma DRM.
- Sistema DRM: uno standard per le implementazioni DRM. I sistemi DRM più comuni includono Apple FairPlay, Google Widevine e Microsoft. PlayReady I sistemi DRM vengono utilizzati dai provider di contenuti per proteggere i contenuti digitali per la distribuzione ai visualizzatori e per l'accesso da parte degli stessi. Per un elenco dei sistemi DRM registrati con DASH-IF, consulta ID di sistema DASH-IF. La specifica DASH-IF CPIX utilizza il termine "sistema DRM" secondo la definizione specificata qui e, in alcuni punti, per indicare ciò a cui questa specifica fa riferimento come piattaforma DRM.
- Soluzione DRM: vedi piattaforma DRM.
- Tecnologia DRM: vedi sistema DRM.
- Encryptor: un componente di elaborazione multimediale che crittografa i contenuti multimediali utilizzando chiavi ottenute dal fornitore delle chiavi. I componenti di crittografia in genere aggiungono anche metadati e segnali di crittografia DRM ai file multimediali. I componenti di crittografia sono in genere codificatori, packager e transcoder.
- Fornitore di chiavi: il componente di una piattaforma DRM che espone un'API REST SPEKE per gestire le richieste di chiavi. Il provider di chiavi potrebbe essere il server di chiavi o potrebbe essere un altro componente della piattaforma.
- Server delle chiavi: il componente di una piattaforma DRM che mantiene le chiavi per la crittografia e la decrittografia dei contenuti.
- Operatore: una persona responsabile del funzionamento dell'intero sistema, inclusi l'crittografo e il fornitore delle chiavi.
- Lettore: un lettore multimediale che opera per conto di uno spettatore. Ottiene le informazioni provenienti da diverse origini, tra cui i file manifest multimediali, i file multimediali e le licenze DRM. Richiede le licenze dalla piattaforma DRM per conto dei visualizzatori.

Onboarding dei clienti

Proteggi i tuoi contenuti dall'uso non autorizzato combinando un provider di chiavi DRM (Digital Rights Management) Secure Packager and Encoder Key Exchange (SPEKE) con il tuo sistema di crittografia e con i tuoi lettori multimediali. SPEKE definisce lo standard per la comunicazione tra i fornitori di chiavi per la gestione dei diritti digitali (DRM) e i fornitori di chiavi per la crittografia e la creazione di pacchetti di contenuti multimediali. Per eseguire l'onboarding, scegli un provider di chiavi della piattaforma DRM e configura la comunicazione tra il provider di chiavi e i componenti di crittografia e i lettori.

Argomenti

Entra a far parte di un fornitore di piattaforme DRM

I seguenti partner Amazon forniscono implementazioni della piattaforma DRM di terze parti per SPEKE. Per ulteriori informazioni sulle offerte e su come contattare, segui i collegamenti alle pagine di Amazon Partner Network. I partner che non dispongono di un link al momento non dispongono di una pagina Amazon Partner Network, ma puoi contattarli direttamente. I partner possono aiutarti a configurare l'utilizzo delle piattaforme.

Fornitore di piattaforme DRM	Supporto per SPEKE v1	Supporto per SPEKE v2 (AWS Elemental) MediaPackage
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKA Entworks	√	√

Fornitore di piattaforme DRM	Supporto per SPEKE v1	Supporto per SPEKE v2 (AWS Elemental) MediaPackage
Insys Cloud DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√
Lettore JW	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	

SPEKE Support nei servizi e prodotti AWS

Questa sezione descrive il supporto SPEKE fornito da AWS Media Services in esecuzione nel cloud AWS e dai prodotti multimediali locali AWS. Questi servizi e prodotti sono i componenti di crittografia nell'architettura di crittografia dei contenuti SPEKE. Verifica che il protocollo di streaming e il sistema DRM desiderati siano disponibili per il servizio o il prodotto.

Servizio o prodotto AWS	Supporto SPEKE v1	Supporto per SPEKE v2	Tecnologie DRM supportate
AWS Elemental MediaConvert : servizio eseguito nel cloud AWS	√		Documentazione

Servizio o prodotto AWS	Supporto SPEKE v1	Supporto per SPEKE v2	Tecnologie DRM supportate
AWS Elemental MediaPackage : servizio eseguito nel cloud AWS	√	√	Documentazione
AWS Elemental Live - Prodotto locale	√		Documentazione: MPEG-DASH/HLS
AWS Elemental Server - Prodotto locale	√		Documentazione

SPEKE Support nei servizi e prodotti dei partner AWS

Questa sezione elenca il supporto SPEKE fornito dai servizi e dai prodotti dei partner AWS eseguiti nel cloud AWS. Questi servizi e prodotti sono i componenti di crittografia nell'architettura di crittografia dei contenuti SPEKE. Verifica che il protocollo di streaming e il sistema DRM desiderati siano disponibili per il servizio o il prodotto.

Servizio o prodotto AWS	Supporto SPEKE v1	Supporto per SPEKE v2	Tecnologie DRM supportate
Codifica video live di Bitmovin	√		Documentazione
Codifica Bitmovin Video on demand (VOD)	√		Documentazione

Specifiche dell'API SPEKE

Questa è la specifica dell'API REST per Secure Packager and Encoder Key Exchange (SPEKE). Usa questa specifica per garantire la protezione del copyright DRM per i clienti che utilizzano la crittografia.

In un flusso di lavoro di streaming di video, il motore di crittografia comunica con il provider di chiavi della piattaforma DRM per richiedere le chiavi di contenuti. Queste chiavi sono altamente sensibili, perciò è fondamentale che il motore di crittografia e il provider di chiavi stabiliscano un canale di comunicazione altamente sicuro e affidabile. È inoltre possibile crittografare le chiavi di contenuto del documento per una crittografia più sicura. end-to-end

Questa specifica affronta i seguenti obiettivi:

- Definire un'interfaccia semplice, affidabile e altamente sicura che i fornitori e i clienti DRM possono utilizzare per integrarsi con i componenti di crittografia quando la crittografia dei contenuti è obbligatoria.
- Copri VOD e i flussi di lavoro in tempo reale e includi le condizioni di errore e i meccanismi di autenticazione necessari per comunicazioni solide e altamente sicure tra i componenti di crittografia e gli endpoint dei provider di chiavi DRM.
- Include il supporto per i pacchetti HLS, MSS e DASH e i relativi sistemi DRM comuni: FairPlay e Widevine/CENC. PlayReady
- Mantieni le specifiche semplici e ampliabili per supportare futuri sistemi DRM.
- Utilizza una semplice API REST.

> **Note**
>
>

O ALTRE RESPONSABILITÀ, DERIVANTI DA, DA O IN CONNESSIONE CON QUESTO MATERIALE O L'USO O ALTRI RAPPORTI DI QUESTO MATERIALE.

Argomenti

Autenticazione

SPEKE richiede l'autenticazione per i prodotti locali e per i servizi e le funzionalità eseguiti nel cloud AWS.

Argomenti

Autenticazione per implementazioni cloud AWS

SPEKE richiede l'autenticazione AWS tramite ruoli IAM per l'utilizzo con un encryptor. I ruoli IAM vengono creati dal provider DRM o dall'operatore che possiede l'endpoint DRM in un account AWS. A ogni ruolo viene assegnato un ARN (Amazon Resource Name), che l'operatore del servizio AWS Elemental fornisce nella console di servizio al momento della richiesta di crittografia. Le autorizzazioni della policy del ruolo devono essere configurate per concedere le autorizzazioni di accesso all'API del provider di chiavi e a nessun'altra risorsa AWS. Quando il componente di crittografia contatta il provider di chiavi DRM, utilizza il ruolo ARN per assumere il ruolo del titolare dell'account del provider di chiavi, che restituisce le credenziali provvisorie al componente di crittografia da utilizzare per accedere al provider di chiavi.

Un'implementazione comune prevede che l'operatore o il fornitore della piattaforma DRM utilizzi Amazon API Gateway davanti al provider principale e quindi abiliti l'autorizzazione AWS Identity and Access Management (AWS IAM) sulla risorsa API Gateway. È possibile utilizzare il seguente esempio di definizione di policy e allegarlo a un nuovo ruolo per concedere le autorizzazioni alla risorsa appropriata. In questo caso, le autorizzazioni sono per tutte le risorse API Gateway:

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

Infine, il ruolo richiede l'aggiunta di una relazione di affidabilità e l'operatore deve essere in grado di selezionare il servizio.

L'esempio seguente mostra un ARN del ruolo creato per accedere al provider di chiavi DRM:

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

Per ulteriori informazioni sulla creazione di un ruolo, consulta AWS AssumeRole. Per ulteriori informazioni sulla firma delle richieste, consulta AWS Sigv4.

Autenticazione per prodotti locali

Per i prodotti locali, consigliamo di utilizzare l'autenticazione digest e SSL/TLS per la sicurezza ottimale, ma almeno è consigliabile utilizzare l'autenticazione di base su HTTPS.

Entrambi i tipi di autenticazione utilizzano l'intestazione `Authorization` nella richiesta HTTP:

- Autenticazione Digest: l'intestazione di autorizzazione è costituita dall'identificatore `Digest` seguito da una serie di valori che autenticano la richiesta. In particolare, un valore di risposta viene generato tramite una serie di funzioni hash MD5 che includono un codice one-time-use nonce univoco proveniente dal server utilizzato per garantire che la password viaggi in modo sicuro.
- Autenticazione di base: l'intestazione di autorizzazione è costituita dall'identificatore `Basic` seguito da una stringa codificata in base 64 che rappresenta il nome utente e la password, separati da due punti.

Per informazioni su autenticazione di base e digest, incluse le informazioni dettagliate sull'intestazione, consulta la specifica Internet Engineering Task Force (IETF) RFC 2617 - Autenticazione HTTP: autenticazione basic e digest per gli accessi.

API SPEKE v1

Per essere conforme a SPEKE, il fornitore di chiavi DRM deve esporre l'API REST descritta in questa specifica. Il componente di crittografia effettua le chiamate API al provider di chiavi.

> **Note**
>
> Il codice di esempio in questa specifica è soltanto indicativo. Non è possibile eseguire gli esempi perché non sono parte di un'implementazione SPEKE completa.

Secure Packager and Encoder Key Exchange utilizza la definizione della struttura dati del DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) per lo scambio di chiavi, con alcune restrizioni. DASH-IF-CPIX definisce uno schema per fornire uno scambio ampliabile multi-DRM dalla piattaforma DRM al componente di crittografia. In questo modo viene abilitata la crittografia dei contenuti per tutti i formati di pacchetti con frequenza di bit adattiva al momento della compressione e della pacchettizzazione dei contenuti. I formati di pacchettizzazione con frequenza di bit adattiva includono HLS, DASH e MSS.

Per informazioni dettagliate sul formato di scambio, consulta la specifica CPIX del DASH Industry Forum all'indirizzo https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf.

Argomenti

- SPEKE API v1 - Personalizzazioni e vincoli alla specifica DASH-IF
- SPEKE API v1 - Componenti di payload standard
- SPEKE API v1 - Esempi di chiamate al metodo Live Workflow
- SPEKE API v1 - Esempi di chiamate al metodo di lavoro VOD
- SPEKE API v1 - Crittografia con chiave di contenuto
- API SPEKE v1 - Heartbeat
- SPEKE API v1 - Sovrascrivere l'identificatore della chiave

SPEKE API v1 - Personalizzazioni e vincoli alla specifica DASH-IF

La specifica DASH-IF CPIX, https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf, supporta una serie di casi d'uso e topologie. La specifica dell'API SPEKE aderisce alla specifica CPIX con le seguenti personalizzazioni e vincoli:

- SPEKE segue il flusso di lavoro di Encryptor Consumer.
- Per le chiavi di contenuto crittografate, SPEKE applica le seguenti restrizioni:
  - SPEKE non supporta la verifica della firma digitale (XMLDSIG) per i payload di richiesta o risposta.
  - SPEKE richiede 2048 certificati basati su RSA.
- Per i flussi di lavoro a chiave rotante, SPEKE richiede il filtro,. `ContentKeyUsageRule` `KeyPeriodFilter` SPEKE ignora tutte le altre impostazioni. `ContentKeyUsageRule`
- SPEKE omette la funzionalità. `UpdateHistoryItemList` Se l'elenco è presente nella risposta, SPEKE lo ignora.
- SPEKE supporta la rotazione dei tasti. SPEKE utilizza solo `ContentKeyPeriod@index per tenere traccia del periodo chiave.
- Per supportare MSS PlayReady, SPEKE utilizza un parametro personalizzato sotto il `DRMSystem` tag,. `SPEKE:ProtectionHeader`
- Per la pacchettizzazione HLS, se `URIExtXKey` è presente nella risposta, deve contenere i dati completi da aggiungere nel parametro URI del tag `EXT-X-KEY` di una playlist HLS, senza ulteriore segnalazione richiesta.
- Per la playlist HLS, sotto il `DRMSystem` tag, SPEKE fornisce i parametri personalizzati opzionali `speke:KeyFormat` `espeke:KeyFormatVersions`, per i valori del tag `KEYFORMAT` e, i `KEYFORMATVERSIONS` parametri. `EXT-X-KEY`

  Il vettore di inizializzazione (IV) HLS segue sempre il numero del segmento, a meno che non sia specificato in modo esplicito dall'operatore.
- Al momento di richiedere le chiavi, il componente di crittografia potrebbe utilizzare l'attributo facoltativo `@explicitIV` dell'elemento `ContentKey`. Il provider di chiavi è in grado di rispondere con un IV utilizzando `@explicitIV`, anche se l'attributo non è incluso nella richiesta.
- Il componente di crittografia crea l'identificatore chiave (`KID`), che rimane uguale per un determinato periodo di chiavi e ID di contenuti. Il provider di chiavi include `KID` nella risposta al documento di richiesta.

- Il provider di chiavi potrebbe includere un valore per l'intestazione della risposta `Speke-User-Agent` per identificarsi per il debug.
- Al momento SPEKE non supporta più tracce o chiavi per contenuto.

  Il criptatore conforme a SPEKE funge da client e invia le operazioni all'endpoint del provider di chiavi. `POST` Il componente di crittografia potrebbe inviare una richiesta `heartbeat` periodica per assicurarsi che la connessione tra il componente di crittografia e l'endpoint del provider di chiavi sia funzionando correttamente.

SPEKE API v1 - Componenti di payload standard

In qualsiasi richiesta SPEKE, il componente di crittografia può richiedere le risposte per uno o più sistemi DRM. Il componente di crittografia specifica i sistemi DRM in `<cpix:DRMSystemList>` del payload della richiesta. Ogni specifica di sistema include la chiave e indica il tipo di risposta da restituire.

L'esempio seguente mostra un elenco dei sistemi DRM con una singolo specifica del sistema DRM:

```
<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>
```

La tabella seguente elenca i componenti principali di ciascun `<cpix:DRMSystem>`.

Identificatore	Descrizione
`systemId` o `schemeId`	Identificatore univoco per il tipo di sistema DRM, così come registrato presso l'organiz zazione DASH IF. Per un elenco, vedi ID dei sistemi DASH-IF.
`kid`	L'ID della chiave . Non è la chiave effettiva, ma un identificatore che punta alla chiave in una tabella hash.

Identificatore	Descrizione
`<cpix:UriExtXKey>`	Richiede una chiave non crittografata standard. Il tipo di risposta della chiave deve essere questa o la risposta PSSH.
`<cpix:PSSH>`	Richiede una Protection System Specific Header (PSSH). Questo tipo di intestazione contiene un riferimento a `kid`, a `systemID` e ai dati personalizzati per il vendor DRM, come parte di Common Encryption (CENC). Il tipo di risposta della chiave deve essere questa o la risposta `UriExtXKey` .

_Richieste di esempio per la chiave standard e per PSSH _

L'esempio seguente mostra parte di una richiesta di esempio dal componente di crittografia al provider di chiavi DRM, con i componenti principali evidenziati. La prima richiesta è per una chiave standard, mentre la seconda richiesta è per una risposta PSSH:

```
<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>
```

_Risposte di esempio per Standard Key e per PSSH _

L'esempio seguente mostra la risposta corrispondente dal provider di chiavi DRM al componente di crittografia:

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

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

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

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

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

SPEKE API v1 - Esempi di chiamate al metodo Live Workflow

Richiedi esempio di sintassi

L'URL seguente è un esempio e non indica un formato fisso:

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

Corpo della richiesta

Elemento CPIX

Intestazioni di richiesta

Nome	Type	Si verifica	Descrizione
`AWS Authorization`	Stringa	1..1	Vedi AWS Sigv4
`X-Amz-Security-Token`	Stringa	1..1	Vedi AWS Sigv4
`X-Amz-Date`	Stringa	1..1	Vedi AWS Sigv4
`Content-Type`	Stringa	1..1	application/xml

Intestazioni di risposta

Nome	Type	Si verifica	Descrizione
`Speke-User-Agent`	Stringa	1..1	Stringa che identifica il provider di chiavi
`Content-Type`	Stringa	1..1	application/xml

Richiesta e risposta

CODICE HTTP	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	Risposta payload DASH-CPIX
`4XX (Client error)`	Messaggio di errore del client	1..1	Descrizione dell'errore del client
`5XX (Server error)`	Messaggio di errore del server	1..1	Descrizione dell'errore del server

> **Note**
>
> Gli esempi di questa sezione non includono la crittografia della chiave dei contenuti. Per informazioni su come aggiungere la crittografia con chiave di contenuto, consulta Content Key encryption.

Payload di richiesta di esempio in tempo reale con chiavi in chiaro

L'esempio seguente mostra un payload tipico della richiesta in tempo reale dal componente di crittografia al provider di chiavi DRM:

```
<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>
```

Payload di risposta di esempio in tempo reale con chiavi in chiaro

Il seguente esempio mostra un payload tipico di risposta dal provider di chiavi DRM:

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

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

```
  </cpix:DRMSystem>

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

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

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

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

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

 <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4IhflQAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAcA
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
```

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

SPEKE API v1 - Esempi di chiamate al metodo di lavoro VOD

Richiedi esempio di sintassi

L'URL seguente è un esempio e non indica un formato fisso.

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

Corpo della richiesta

Elemento CPIX

Intestazioni di risposta

Nome	Type	Si verifica	Descrizione
`Speke-User-Agent`	Stringa	1..1	Stringa che identifica il provider di chiavi
`Content-Type`	Stringa	1..1	application/xml

Richiesta e risposta

CODICE HTTP	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	Risposta payload DASH-CPIX
`4XX (Client error)`	Messaggio di errore del client	1..1	Descrizione dell'errore del client
`5XX (Server error)`	Messaggio di errore del server	1..1	Descrizione dell'errore del server

> **Note**
>
> Gli esempi di questa sezione non includono la crittografia della chiave dei contenuti. Per informazioni su come aggiungere la crittografia con chiave di contenuto, consulta Content Key encryption.

Payload di richiesta di esempio VOD con chiavi in chiaro

L'esempio seguente mostra un payload tipico della richiesta VOD di base dal componente di crittografia al provider di chiavi DRM:

```
<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>
```

Payload di risposta di esempio VOD con chiavi in chiaro

Il seguente esempio mostra un payload VOD di base di risposta dal provider di chiavi DRM:

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

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

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

 <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIExtXKey>
   <speke:KeyFormat>Y29tLmFwcGxlLnN0cmVhbWluZ2tleWRlbGl2ZXJ5</speke:KeyFormat>
```

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

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

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

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

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

SPEKE API v1 - Crittografia con chiave di contenuto

Facoltativamente, puoi aggiungere la crittografia con chiave di contenuto all'implementazione SPEKE. La crittografia delle chiavi di contenuto garantisce una end-to-end protezione completa crittografando le chiavi di contenuto per il transito, oltre alla crittografia del contenuto stesso. Se non la implementate per il vostro fornitore di chiavi, vi affidate alla crittografia a livello di trasporto e all'autenticazione avanzata per la sicurezza.

Per utilizzare la crittografia a chiave di contenuto per gli crittografi in esecuzione nel cloud AWS, i clienti importano i certificati in AWS Certificate Manager e quindi utilizzano gli ARN dei certificati risultanti per le loro attività di crittografia. L'encryptor utilizza gli ARN dei certificati e il servizio ACM per fornire chiavi di contenuto crittografate al fornitore di chiavi DRM.

Restrizioni

SPEKE supporta la crittografia delle chiavi di contenuto come specificato nella specifica DASH-IF CPIX con le seguenti restrizioni:

- SPEKE non supporta la verifica della firma digitale (XMLDSIG) per i payload di richiesta o risposta.
- SPEKE richiede 2048 certificati basati su RSA.

Queste restrizioni sono elencate anche in Personalizzazioni e vincoli alla specifica DASH-IF.

Implementazione della crittografia delle chiavi di contenuti

Per offrire la crittografia delle chiavi dei contenuti, includere quanto segue nelle implementazioni del provider di chiavi DRM:

- Gestire l'elemento `<cpix:DeliveryDataList>` nei payload della richiesta e della risposta.
- Fornire i valori crittografati nel `<cpix:ContentKeyList>` dei payload della risposta.

Per ulteriori informazioni su questi elementi, consulta la specifica DASH-IF CPIX 2.0.

Elemento di crittografia della chiave dei contenuti di esempio `<cpix:DeliveryDataList>` nel payload della richiesta

L'esempio seguente evidenzia l'elemento `<cpix:DeliveryDataList>` aggiunto in grassetto:

```
<?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>
```

Elemento di crittografia della chiave dei contenuti di esempio `<cpix:DeliveryDataList>` nel payload della risposta

L'esempio seguente evidenzia l'elemento `<cpix:DeliveryDataList>` aggiunto in grassetto:

```
<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>
```

Elemento di crittografia della chiave dei contenuti di esempio `<cpix:ContentKeyList>` nel payload della risposta

L'esempio seguente mostra la gestione della chiave dei contenuti crittografati nell'elemento `<cpix:ContentKeyList>` del payload di risposta. Questo utilizza l'elemento `<pskc:EncryptedValue>`:

```
   <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>
```

In base al confronto, l'esempio seguente mostra un payload di risposta simile con la chiave di contenuti distribuita non crittografata, come chiave in chiaro. Questo utilizza l'elemento `<pskc:PlainValue>`:

```
   <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>
```

API SPEKE v1 - Heartbeat

Richiedi esempio di sintassi

L'URL seguente è un esempio e non indica un formato fisso:

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

Richiesta e risposta

CODICE HTTP	Nome payload	Si verifica	Descrizione
`200 (Success)`	statusMessage	1..1	Messaggio che descrive lo stato

SPEKE API v1 - Sovrascrivere l'identificatore della chiave

Il componente di crittografia crea un nuovo identificatore chiave (KID) che ruota le chiavi. Trasferisce il KID al provider di chiavi DRM nelle richieste. Quasi sempre, il provider di chiavi risponde utilizzando lo stesso KID, ma è in grado di fornire un valore diverso per il KID nella risposta.

Di seguito è riportato un esempio di richiesta con il 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>
```

La seguente risposta sovrascrive il KID in `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>
```

API SPEKE v2

Per essere conforme a SPEKE, il fornitore di chiavi DRM deve esporre l'API REST descritta in questa specifica. Il componente di crittografia effettua le chiamate API al provider di chiavi.

> **Note**
>
> Il codice di esempio in questa specifica è soltanto indicativo. Non è possibile eseguire gli esempi perché non sono parte di un'implementazione SPEKE completa.

Secure Packager and Encoder Key Exchange utilizza la definizione della struttura dati del DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) per lo scambio di chiavi, con alcune restrizioni. DASH-IF-CPIX definisce uno schema per fornire uno scambio ampliabile multi-DRM dalla piattaforma DRM al componente di crittografia. In questo modo viene abilitata la crittografia dei contenuti per tutti i formati di pacchetti con frequenza di bit adattiva al momento della compressione e della pacchettizzazione dei contenuti. I formati di pacchettizzazione con frequenza di bit adattiva includono HLS, DASH e MSS.

A partire dalla versione 2.0, SPEKE è allineato a una versione CPIX specifica:

Sul lato SPEKE, questo viene applicato tramite l'uso dell'intestazione `X-Speke-Version` HTTP e sul lato CPIX tramite l'uso dell'attributo. `CPIX@version` La mancanza di questi elementi nelle richieste

è tipica dei flussi di lavoro precedenti di SPEKE v1. Nei flussi di lavoro SPEKE v2, ci si aspetta che il provider chiave elabori i documenti CPIX solo se supporta entrambi i parametri di versione.

Per informazioni dettagliate sul formato di scambio, consulta la specifica CPIX 2.3 del DASH Industry Forum.

Nel complesso, SPEKE v2.0 apporta le seguenti evoluzioni rispetto a SPEKE v1.0:

- Tutti i tag dello spazio dei nomi XML SPEKE sono obsoleti a favore dei tag equivalenti nello spazio dei nomi XML CPIX
- `SPEKE:ProtectionHeader` è obsoleto e sostituito da `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`, `SPEKE:KeyFormat` e `SPEKE:KeyFormatVersions` sono obsoleti e sostituiti da `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id` è sostituito da `CPIX@contentId`
- Nuovi attributi CPIX obbligatori:, `CPIX@version` `ContentKey@commonEncryptionScheme`
- Nuovo elemento CPIX opzionale: `DRMSystem.ContentProtectionData`
- Support per più chiavi di contenuto
- Meccanismo di controllo incrociato tra SPEKE e CPIX
- Evoluzione delle intestazioni HTTP: nuova intestazione, intestazione rinominata in `X-Speke-Version` `Speke-User-Agent` `X-Speke-User-Agent`
- Deprecazione dell'API Heartbeat

Poiché la specifica SPEKE v1.0 rimane invariata, non è necessario modificare le implementazioni esistenti per continuare a supportare i flussi di lavoro SPEKE v1.0.

Argomenti

- SPEKE API v2 - Personalizzazioni e vincoli alla specifica DASH-IF
- SPEKE API v2 - Componenti di payload standard
- SPEKE API v2 - Contratto di crittografia
- SPEKE API v2 - Esempi di chiamate al metodo Live Workflow
- SPEKE API v2 - Esempi di chiamate al metodo di lavoro VOD
- SPEKE API v2 - Crittografia delle chiavi del contenuto
- SPEKE API v2 - Sovrascrivere l'identificatore chiave

SPEKE API v2 - Personalizzazioni e vincoli alla specifica DASH-IF

La specifica CPIX 2.3 del DASH Industry Forum supporta una serie di casi d'uso e topologie. La specifica SPEKE API v2.0 definisce sia un profilo CPIX che un'API per CPIX. Per raggiungere questi due obiettivi, aderisce alla specifica CPIX con le seguenti personalizzazioni e vincoli:

Profilo CPIX

- SPEKE segue il flusso di lavoro di Encryptor Consumer.
- Per le chiavi di contenuto crittografate, SPEKE applica le seguenti restrizioni:
  - SPEKE non supporta la verifica della firma digitale (XMLDSIG) per i payload di richiesta o risposta.
  - SPEKE richiede 2048 certificati basati su RSA.
- SPEKE sfrutta solo un sottoinsieme di funzionalità CPIX:
  - SPEKE `UpdateHistoryItemList` omette la funzionalità. Se l'elenco è presente nella risposta, SPEKE lo ignora.
  - SPEKE omette la funzionalità dei tasti root/leaf. Se l'`ContentKey@dependsOnKey`attributo è presente nella risposta, SPEKE lo ignora.
  - SPEKE omette l'`BitrateFilter`elemento e l'attributo. `VideoFilter@wcg` Se questi elementi o attributi sono presenti nel payload CPIX, SPEKE lo ignora.
- Solo gli elementi o gli attributi indicati come «Supportati» nella pagina Standard Payload Components o nella pagina del contratto di crittografia possono essere utilizzati nei documenti CPIX scambiati con SPEKE v2.
- Se inclusi in una richiesta CPIX dal criptatore, tutti gli elementi e gli attributi devono riportare un valore valido nella risposta CPIX del fornitore di chiavi. In caso contrario, l'encryptor si fermerà e genererà un errore.
- SPEKE supporta la rotazione dei tasti con gli elementi. `KeyPeriodFilter` SPEKE utilizza solo il `ContentKeyPeriod@index` per tenere traccia del periodo chiave.
- Per la segnalazione HLS, devono essere utilizzati più `DRMSystem.HLSSignalingData` elementi: uno con il valore di `DRMSystem.HLSSignalingData@playlist` attributo 'media' e l'altro con il valore di `DRMSystem.HLSSignalingData@playlist` attributo 'master'.
- Al momento di richiedere le chiavi, il componente di crittografia potrebbe utilizzare l'attributo facoltativo `@explicitIV` dell'elemento `ContentKey`. Il provider di chiavi è in grado di rispondere con un IV utilizzando `@explicitIV`, anche se l'attributo non è incluso nella richiesta.

- Il componente di crittografia crea l'identificatore chiave (`KID`), che rimane uguale per un determinato periodo di chiavi e ID di contenuti. Il provider di chiavi include `KID` nella risposta al documento di richiesta.
- L'encryptor deve includere un valore per l'attributo. `CPIX@contentId` Quando riceve un valore vuoto per questo attributo, il fornitore della chiave restituirà un errore con la descrizione 'Missing CPIX @contentId '. `CPIX@contentId`il valore non può essere sovrascritto dal fornitore di chiavi.

  `CPIX@id`il valore, se non nullo, deve essere ignorato dal fornitore della chiave.
- L'encryptor deve includere un valore per l'attributo. `CPIX@version` Quando riceve un valore vuoto per questo attributo, il fornitore della chiave restituirà un errore con la descrizione 'Missing CPIX @version '. Quando si riceve una richiesta con una versione non supportata, la descrizione dell'errore restituita dal fornitore della chiave è «Unsupported CPIX @version».

  `CPIX@version`il valore non può essere sovrascritto dal fornitore della chiave.
- L'encryptor deve includere un valore per l'`ContentKey@commonEncryptionScheme`attributo per ogni chiave richiesta. Quando riceve un valore vuoto per questo attributo, il fornitore della chiave restituirà un errore con la descrizione 'Missing ContentKey @ commonEncryptionScheme for KID '. `id`

  Un documento CPIX unico non può combinare più valori per attributi diversi. `ContentKey@commonEncryptionScheme` Quando riceve una tale combinazione, il fornitore della chiave restituirà un errore con la descrizione «Combinazione @ non conforme ContentKey». commonEncryptionScheme

  Non tutti i `ContentKey@commonEncryptionScheme` valori sono compatibili con tutte le tecnologie DRM. Quando riceve una tale combinazione, il fornitore della chiave restituirà un errore con la descrizione 'ContentKey@ commonEncryptionScheme non compatibile con `id` DRMSystem'.

  `ContentKey@commonEncryptionScheme`il valore non può essere sovrascritto dal fornitore della chiave.
- Quando riceve valori diversi per `DRMSystem@PSSH` un `<pssh>` elemento `DRMSystem.ContentProtectionData` innerXML nel corpo della risposta CPIX, l'encryptor si interrompe e genera un errore.

API per CPIX

- Il fornitore di chiavi deve includere un valore per l'intestazione della risposta `X-Speke-User-Agent` HTTP.
- Un crittografo conforme a SPEKE funge da client e invia operazioni POST all'endpoint del provider di chiavi.
- Il criptatore deve includere un valore per l'intestazione della richiesta `X-Speke-Version` HTTP, con la versione SPEKE utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, come '2.0' per SPEKE v2.0. Se il fornitore di chiavi non supporta la versione SPEKE utilizzata dall'encryptor per la richiesta corrente, restituirà un errore con la descrizione «Versione SPEKE non supportata» e non tenterà di elaborare il documento CPIX con la massima diligenza.

  Il valore dell'`X-Speke-Version`intestazione definito dall'encoder non può essere modificato dal fornitore della chiave nella risposta alla richiesta.
- Quando riceve errori nel corpo della risposta, il criptatore deve generare un errore e non riprovare la richiesta con una versione SPEKE v1.0.

  Se il fornitore di chiavi non restituisce un errore ma non riesce a restituire un documento CPIX che include le informazioni obbligatorie, il criptatore dovrebbe fermarsi e generare un errore.

La tabella seguente riassume i messaggi standard che devono essere restituiti dal fornitore di chiavi nel corpo del messaggio. Il codice di risposta HTTP in caso di errore deve essere un 4XX o un 5XX, mai un 200. Il codice di errore 422 può essere utilizzato per tutti gli errori relativi a SPEKE/CPIX.

Caso di errore	Messaggio di errore
CPIX @contentId non è definito	CPIX @contentId mancante
CPIX @version non è definito	CPIX @version mancante
CPIX @version non è supportato	CPIX @version non supportato
ContentKey@ commonEncryptionScheme non è definito	ContentKey@ mancante commonEncryptionScheme per KID `id` (dove è `id` uguale al valore ContentKey @kid)

Caso di errore	Messaggio di errore
Più commonEncryptionScheme valori ContentKey @ utilizzati in un singolo documento CPIX	Combinazione @ non conforme ContentKey commonEncryptionScheme
ContentKey@ non commonEncryptionScheme è compatibile con la tecnologia DRM	ContentKey@ commonEncryptionScheme non compatibile con DRMSystem `id` (dove è `id` uguale al valore DRMSystem @systemId)
Il valore dell'intestazione X-Speke-Version non è una versione SPEKE supportata	Versione SPEKE non supportata
Il contratto di crittografia non è valido	Contratto di crittografia non valido
Il contratto di crittografia contraddice i vincoli relativi ai livelli di sicurezza del DRM	Il contratto di crittografia CPIX richiesto non è supportato
Il contratto di crittografia non include alcun elemento or VideoFilter AudioFilter	Contratto di crittografia CPIX mancante

SPEKE API v2 - Componenti di payload standard

Tramite una singola richiesta SPEKE, il criptatore può richiedere più chiavi di contenuto, insieme alla necessaria segnalazione Manfest per più formati di packaging, in base al contratto di crittografia definito per un determinato contenuto.

Per coprire tutti questi aspetti, un documento CPIX standard è composto da tre sezioni di elenco obbligatorie, più una sezione opzionale per la rotazione delle chiavi relative ai contenuti in tempo reale.

<cpix:CPIX><cpix: ContentKeyList > sezione ed elemento di primo livello

Questa è una sezione obbligatoria, rilevante sia per lo streaming Live che per lo streaming VOD, che definisce le diverse chiavi di contenuto che devono essere utilizzate dal criptatore. L'`<cpix:ContentKeyList>`elemento può contenere uno o più elementi `<cpix:ContentKey>` secondari, ognuno dei quali descrive una chiave di contenuto distinta.

Secondo la specifica CPIX, i possibili valori dell'`ContentKey@commonEncryptionScheme`attributo sono definiti nella specifica Common encryption in ISO Base Media File Format Files (ISO/IEC 23001-7:2016):

- 'cenc': campionamento completo in modalità AES-CTR e crittografia video NAL Subsample
- 'cbc1': campionamento completo in modalità AES-CBC e crittografia del sottocampione video NAL
- 'cens': crittografia del pattern NAL video parziale in modalità AES-CTR
- 'cbcs': crittografia del pattern NAL video parziale in modalità AES-CBC

L'esempio seguente mostra un documento CPIX con un'unica chiave di contenuto non crittografata:

```
<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>
```

Per impostazione predefinita, le chiavi di contenuto non sono crittografate, come nell'esempio seguente. Tuttavia, la crittografia delle chiavi di contenuto può essere richiesta dal criptatore mediante l'inclusione dell'elemento<cpix : >. DeliveryDataList Per ulteriori dettagli, consulta la sezione Content Key Encryption.

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
<cpix:CPIX>	ContentID, versione, xmlns: cpix, xmlns: pskc	nome, xmlns:enc	uno <cpix: ContentKeyList >, uno<cpix:	uno <cpix: DeliveryDataList >ContentK

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
			DRM >, uno <cpix : >SystemListContentKeyUsageRuleList	eyPeriodList, uno <cpix : >
<cpixContentKeyList: >	-	id	almeno un <cpix : >ContentKey	-
<cpix : >ContentKey	ragazzo, Dati commonEncryptionScheme	id, Algoritmo, ExplicitIV	uno <pskc:Secret>	-
<pskc:Secret>	PlainValue o EncryptedValue	valore MAC	-	<enc: EncryptionMethod >, <enc : >CipherData

SystemList<cpix:DRM >sezione

Questa è una sezione obbligatoria, rilevante sia per lo streaming live che per quello VOD, che definisce i diversi sistemi DRM che devono essere sfruttati insieme alle chiavi di contenuto.

L'esempio seguente mostra un elenco di sistemi DRM con una singola PlayReady specifica del sistema DRM:

```
<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>
```

Per un elenco completo dei SystemID DRM, consulta la sezione Protezione dei contenuti dell'archivio DASH-IF Identifiers.

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
<cpix:DRMSystemList>	-	id	almeno uno <cpix:DRMSystem>	-
<cpix:DRMSystem>	ragazzo, SystemID	id, nome, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHeaderData, due <cPix:hlsSignalingData > elementi con un valore di attributo di playlist diverso

`DRMSystem@PSSH`è obbligatorio se l'incapsulamento ISO-BMFF viene applicato ai segmenti multimediali. `DRMSystem.ContentProtectionData`L'`<pssh>`elemento InnerXML viene utilizzato dal criptatore solo per scopi di segnalazione manifesta.

Se `DRMSystem@PSSH` è presente e `DRMSystem.ContentProtectionData` contiene un elemento innerXML`<pssh>`, entrambi i valori devono essere identici.

Se la `DRMSystem` segnalazione deve essere trasmessa nei manifesti HLS, nella richiesta `<cpix:HLSSignalingData playlist="media">` e nella risposta CPIX devono essere inclusi sia `<cpix:HLSSignalingData playlist="master">` gli elementi a che a.

ContentKeyPeriodListSezione <cpix : >

Questa è una sezione facoltativa, rilevante solo per lo streaming live, che definisce i periodi crittografici applicati al contenuto.

L'`<cpix:ContentKeyPeriodList>`elemento può contenere uno o più elementi `<cpix:ContentKeyPeriod>` secondari, ognuno dei quali descrive un periodo crittografico distinto nella timeline live. L'uso degli UUID come parte del valore dell'attributo id è un approccio comunemente usato.

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

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
<cpix : >ContentKeyPeriodList	-	id	almeno un <cpix : >ContentKeyPeriod	-
<cpix : >ContentKeyPeriod	id, indice	-	-	-

Se vengono utilizzati periodi crittografici, le chiavi di crittografia devono essere allegate anche a uno dei periodi crittografici nel documento CPIX, come mostrato nella sezione seguente.

Sezione <cpix : >ContentKeyUsageRuleList

Questa è una sezione obbligatoria, rilevante sia per lo streaming live che per quello VOD, che definisce in che modo le diverse chiavi di contenuto proteggeranno le tracce all'interno dello streamset e durante i periodi crittografici.

L'elemento <cpix: ContentKeyUsageRuleList > può contenere uno o più elementi secondari <cpix: ContentKeyUsageRule >, ognuno dei quali descrive le tracce a cui l'encryptor applica una

determinata chiave di contenuto, potenzialmente durante uno specifico periodo di crittografia. È necessario che almeno un elemento <cpix: AudioFilter > o un elemento <cpix : >sia presente in un elemento<cpix : >. VideoFilter ContentKeyUsageRule

L'esempio seguente mostra un elenco semplice con una sola regola che applica una singola chiave di contenuto a tutte le tracce audio e video durante uno specifico periodo crittografico.

```
<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>
```

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
<cpix : >ContentKeyUsageRuleList	-	id	almeno un <cpix : >ContentKeyUsageRule	-
<cpix : >ContentKeyUsageRule	bambino, intendedTrackType	-	almeno un <cpix: AudioFilter > o un <cpix : >(*) VideoFilter	<cpix : >KeyPeriodFilter
<cpix : >KeyPeriodFilter	Periodo ID	-	-	-
<cpix : >AudioFilter	-	MinChannels, MaxChannels	-	-
<cpix : >VideoFilter	-	minPixels, maxPixels,	-	-

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
		hdr, minFPS, maxFPS		

(*) Per una spiegazione dettagliata sull'uso di una o più chiavi di contenuto per proteggere una o più tracce in uno streamset, consulta la sezione relativa alla documentazione del contratto di crittografia.

_

SPEKE API v2 - Contratto di crittografia

Il contratto di crittografia definisce quali chiavi di contenuto proteggono quali tracce all'interno di un determinato streamset, in base alle caratteristiche delle tracce.

L'utilizzo di più chiavi di contenuto per diverse tracce in uno streamset, nonostante sia una best practice consigliata del settore, non è obbligatorio, ma consigliato: almeno due chiavi di contenuto diverse, una per le tracce audio e una per le tracce video. L'utilizzo di un'unica chiave di contenuto per crittografare più tracce è possibile, ma deve essere segnalato esplicitamente nel documento CPIX inviato dal criptatore al fornitore delle chiavi. In generale, il criptatore descrive sempre con precisione quante chiavi di contenuto sono necessarie e come vengono sfruttate per crittografare le varie tracce multimediali.

Principi

Il contratto di crittografia si trova nella `<cpix:ContentKeyUsageRuleList>` sezione del documento CPIX. In questa sezione, ogni chiave di contenuto definita nella `<cpix:ContentKeyList>` sezione corrisponde a un `<cpix:ContentKeyUsageRule>` elemento specifico, che deve includere:

- un `ContentKeyUsageRule@intendedTrackType` attributo che può fare riferimento a uno o più sottocomponenti, separati dal segno «+» se vengono utilizzati più sottocomponenti. Il valore di `ContentKeyUsageRule@intendedTrackType` deve essere unico in un contratto di crittografia e non può essere utilizzato in più `ContentKeyUsageRule` elementi.
- uno o più elementi `<cpix:AudioFilter>` o `<cpix:VideoFilter>` un elemento secondario, a seconda del valore dell'`ContentKeyUsageRule@intendedTrackType`attributo.

Le regole che regolano questa relazione sono le seguenti:

- Quando tutte le tracce audio e video dello streamset devono essere protette con una chiave di contenuto univoca, è `'ALL'` necessario utilizzare la stringa come valore dell'`ContentKeyUsageRule@intendedTrackType`attributo. L'esempio 1 mostra un caso d'uso di questo tipo. In questa situazione, devono essere inclusi sia gli elementi a che gli elementi `<cpix:VideoFilter />` secondari senza alcun attributo. `<cpix:AudioFilter />` Qualsiasi altra combinazione di `<cpix:AudioFilter>` e/o `<cpix:VideoFilter>` elementi non è valida in questo particolare contesto.
- Per tutti gli altri casi d'uso, il valore dell'`ContentKeyUsageRule@intendedTrackType`attributo può essere definito liberamente e il numero di elementi `<cpix:VideoFilter />` secondari `<cpix:AudioFilter />` e uno devono corrispondere al numero di sottocomponenti aggregati tramite il segno '+'. Gli esempi 2/3/4/5/6/7/9/10 illustrano questo requisito, quando nel valore dell'attributo è presente un singolo sottocomponente. `ContentKeyUsageRule@intendedTrackType` L'esempio 8 lo illustra quando vengono utilizzati più sottocomponenti: `ContentKeyUsageRule@intendedTrackType="SD +HD"` è descritto da due elementi figlio distinti con valori di attributi diversi ed `ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"` è descritto da tre elementi `<cpix:VideoFilter>` figlio distinti con valori di attributi diversi. `<cpix:VideoFilter>`

Filtri

CPIX definisce più elementi e attributi di filtraggio, ma SPEKE ne supporta solo un sottoinsieme. La tabella seguente riassume queste differenze:

Tipo di filtro CPIX	Supporto generale per SPEKE	Attributi di filtro supportati da SPEKE	Attributi di filtro non supportati da SPEKE
<cpix : >VideoFilter	Sì	minPixels, maxPixels, hdr, minFPS, maxFPS (attributi opzionali)	wcg
<cpix : >AudioFilter	Sì	minChannels, maxChannels (attributi opzionali)	

Tipo di filtro CPIX	Supporto generale per SPEKE	Attributi di filtro supportati da SPEKE	Attributi di filtro non supportati da SPEKE
<cpix : >KeyPeriodFilter	Sì	perioDid (attributo obbligatorio)	
<cpix : >BitrateFilter	No	N/D	N/D
<cpix : >LabelFilter	No	N/D	N/D

Secondo la specifica CPIX per VideoFilter, [MinPixels, MaxPixels] è un intervallo completo in entrambe le dimensioni, mentre (MinFPS, MaxFPS] è incluso solo per la dimensione MaxFPS. Infatti AudioFilter, [minChannels, maxChannels] è un intervallo inclusivo in entrambe le dimensioni.

Situazioni problematiche

Vi sono situazioni in cui le informazioni fornite nel contratto di crittografia potrebbero essere parziali, ambigue o errate. In questi casi, è importante che il criptatore e il fornitore della chiave si comportino in modo appropriato e garantiscano un'adeguata protezione dei contenuti. La tabella seguente presenta il comportamento consigliato in queste situazioni:

In questa situazione	Il criptatore dovrebbe/deve...	Il fornitore delle chiavi dovrebbe/deve...
Nessuna regola si applica a una o più tracce nello streamset (vedi esempio 3 di seguito)	Il criptatore dovrebbe esaminare la sua configurazione (esterna al payload CPIX) e verificare che le tracce interessate non richiedano la crittografia. Se non è previsto, l'encryptor dovrebbe generare un errore e interrompere l'elaborazione.	Non rilevante: il fornitore delle chiavi non conosce la struttura dello streamset.
Diverse regole si sovrappongono e suggeriscono più chiavi di contenuto per	Il criptatore deve applicare l'ultima valuta valutata ContentKeyUsageRule con	Non pertinente: il fornitore di chiavi non conosce la struttura dello streamset.

In questa situazione	Il criptatore dovrebbe/deve...	Il fornitore delle chiavi dovrebbe/deve...
crittografare una traccia specifica	successo nell'ordine del documento.	
Il contratto di crittografia cambia in un singolo ciclo di richiesta/risposta SPEKE	Il criptatore deve sollevare un'eccezione e interrompere l'elaborazione, in quanto il fornitore della chiave non è responsabile della definizione del contratto di crittografia.	Per evitare che questa situazione si verifichi in primo luogo, il fornitore di chiavi non deve modificare un contratto di crittografia ricevuto nel payload CPIX della richiesta SPEKE.
Contratto di crittografia non valido: eccezione del vincolo di cardinalità intendedT rackType /Filters, filtri o attributi non supportati	Il sistema di crittografia deve sollevare un'eccezione, interrompere l'elaborazione e non inviare la richiesta SPEKE al fornitore della chiave, poiché molto probabilmente comporterebbe una protezion e errata dei contenuti o lascerebbe alcune tracce non protette.	Il fornitore di chiavi deve sollevare un'eccezione e restituire un errore «Contratto di crittografia non valido».
Contratto di crittografia ben strutturato, ma che viola i vincoli dei livelli di sicurezza DRM: ad esempio, viene richiesta un'unica chiave di contenuto per proteggere sia le tracce audio che le tracce video UHD	Se l'autore della crittografia è a conoscenza dei vincoli dei livelli di sicurezza del DRM, dovrebbe sollevare un'eccezi one, interrompere l'elabora zione e non inviare la richiesta SPEKE al fornitore delle chiavi, poiché molto probabilm ente comporterebbe una protezione errata dei contenuti .	Il fornitore di chiavi deve sollevare un'eccezione e restituire l'errore «Contratto di crittografia CPIX richiesto non supportato».

In questa situazione	Il criptatore dovrebbe/deve...	Il fornitore delle chiavi dovrebbe/deve...
Contratto di crittografia mancante	Il criptatore non deve inviare documenti CPIX che non contengano alcun elemento or. VideoFilter AudioFilter	Il fornitore della chiave deve sollevare un'eccezione e restituire l'errore «Contratto di crittografia CPIX mancante».

Esempi di contratti di crittografia

Esempio 1: una chiave di contenuto per tutte le tracce audio e video

```
<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>
```

Esempio 2: una chiave di contenuto per tutte le tracce video, una chiave di contenuto per tutte le tracce audio

```
<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>
```

Esempio 3: una chiave di contenuto per tutte le tracce video, tracce audio non crittografate

```
<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>
```

Esempio 4: più chiavi di contenuto per diverse tracce video (SD/HD), una chiave di contenuto per tutte le tracce audio

```
<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>
```

Esempio 5: più chiavi di contenuto per diverse tracce video (SD/HD/UHD), una chiave di contenuto per tutte le tracce audio

```
<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>
```

Esempio 6: più chiavi di contenuto per diverse tracce video (SD/HD/UHD1/UHD2), una chiave di contenuto per tutte le tracce audio

```
<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>
```

Esempio 7: più chiavi di contenuto per diverse tracce video (SD/HD1/HD2/UHD1/UHD2), una chiave di contenuto per tutte le tracce audio

```
<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>
```

Esempio 8: più chiavi di contenuto per diverse tracce video (basate su più tipi di attributi), una chiave di contenuto per tutte le tracce audio

```
<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>
```

Esempio 9: una chiave di contenuto per tutte le tracce video, più chiavi di contenuto per le tracce audio stereo e multicanale

```
<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>
```

Esempio 10: una chiave di contenuto per tutte le tracce video, più chiavi di contenuto per le tracce stereo e due tipi di tracce audio multicanale

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

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

SPEKE API v2 - Esempi di chiamate al metodo Live Workflow

Richiedi esempio di sintassi

L'URL seguente è un esempio e non indica un formato fisso:

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

Corpo della richiesta

Un documento CPIX.

Intestazioni di richiesta

Nome	Type	Si verifica	Descrizione
`AWS Authorization`	Stringa	1..1	Vedi AWS Sigv4
`X-Amz-Security-Token`	Stringa	1..1	Vedi AWS Sigv4
`X-Amz-Date`	Stringa	1..1	Vedi AWS Sigv4
`Content-Type`	Stringa	1..1	application/xml
`X-Speke-Version`	Stringa	1..1	Versione dell'API SPEKE utilizzata con la richiesta, formulata come. MajorVersion MinorVersion,

Nome	Type	Si verifica	Descrizione
			ad esempio '2.0' per SPEKE v2.0

Intestazioni di risposta

Nome	Type	Si verifica	Descrizione
`X-Speke-User-Agent`	Stringa	1..1	Stringa che identifica il provider di chiavi
`Content-Type`	Stringa	1..1	application/xml
`X-Speke-Version`	Stringa	1..1	Versione dell'API SPEKE utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, ad esempio '2.0' per SPEKE v2.0

Richiesta e risposta

CODICE HTTP	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	Risposta payload DASH-CPIX
`4XX (Client error)`	Messaggio di errore del client	1..1	Descrizione dell'errore del client
`5XX (Server error)`	Messaggio di errore del server	1..1	Descrizione dell'errore del server

> **Note**
>
> Gli esempi di questa sezione non includono la crittografia della chiave dei contenuti. Per informazioni su come aggiungere la crittografia con chiave di contenuto, vedi Crittografia con chiave di contenuto.

Payload di richiesta di esempio in tempo reale con chiavi in chiaro

L'esempio seguente mostra un tipico payload di richieste live dall'encryptor al provider di chiavi DRM, con una chiave di contenuto per tutte le tracce video e una chiave di contenuto per tutte le tracce audio:

```
<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>
```

Payload di risposta di esempio in tempo reale con chiavi in chiaro

L'esempio seguente mostra un tipico payload di risposta fornito dal fornitore di chiavi DRM (i valori restituiti sono stati abbreviati con [...] per motivi di leggibilità):

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

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

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

SPEKE API v2 - Esempi di chiamate al metodo di lavoro VOD

Richiedi esempio di sintassi

L'URL seguente è un esempio e non indica un formato fisso.

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

Corpo della richiesta

Un documento CPIX.

Intestazioni di richiesta

Nome	Type	Si verifica	Descrizione
`AWS Authorization`	Stringa	1..1	Vedi AWS Sigv4
`X-Amz-Security-Token`	Stringa	1..1	Vedi AWS Sigv4
`X-Amz-Date`	Stringa	1..1	Vedi AWS Sigv4
`Content-Type`	Stringa	1..1	application/xml
`X-Speke-Version`	Stringa	1..1	Versione dell'API SPEKE utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, ad esempio '2.0' per SPEKE v2.0

Intestazioni di risposta

Nome	Type	Si verifica	Descrizione
`X-Speke-User-Agent`	Stringa	1..1	Stringa che identifica il provider di chiavi
`Content-Type`	Stringa	1..1	application/xml
`X-Speke-Version`	Stringa	1..1	Versione dell'API SPEKE utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, ad esempio '2.0' per SPEKE v2.0

Richiesta e risposta

CODICE HTTP	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	Risposta payload DASH-CPIX
`4XX (Client error)`	Messaggio di errore del client	1..1	Descrizione dell'errore del client
`5XX (Server error)`	Messaggio di errore del server	1..1	Descrizione dell'errore del server

> **Note**
>
> Gli esempi di questa sezione non includono la crittografia della chiave dei contenuti. Per informazioni su come aggiungere la crittografia con chiave di contenuto, vedi Crittografia con chiave di contenuto.

Payload di richiesta di esempio VOD con chiavi in chiaro

L'esempio seguente mostra un tipico payload di richieste VOD dall'encryptor al provider di chiavi DRM, con una chiave di contenuto per tutte le tracce video e una chiave di contenuto per tutte le tracce audio:

```
<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>
```

Payload di risposta di esempio VOD con chiavi in chiaro

L'esempio seguente mostra un tipico payload di risposta del fornitore di chiavi DRM (i valori restituiti sono stati abbreviati con [...] per motivi di leggibilità):

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

```
  </cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>h3toSFIlyAYpfXVQ795m6x==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
   <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
   <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
  </cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
   <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
```

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

SPEKE API v2 - Crittografia delle chiavi del contenuto

Facoltativamente, puoi aggiungere la crittografia con chiave di contenuto all'implementazione SPEKE. La crittografia delle chiavi di contenuto garantisce una end-to-end protezione completa crittografando le chiavi di contenuto per il transito, oltre alla crittografia del contenuto stesso. Se non la implementate per il vostro fornitore di chiavi, vi affidate alla crittografia a livello di trasporto e all'autenticazione avanzata per la sicurezza.

Per utilizzare la crittografia a chiave di contenuto per gli crittografi in esecuzione nel cloud AWS, i clienti importano i certificati in AWS Certificate Manager e quindi utilizzano gli ARN dei certificati risultanti per le loro attività di crittografia. L'encryptor utilizza gli ARN dei certificati e il servizio ACM per fornire chiavi di contenuto crittografate al fornitore di chiavi DRM.

Restrizioni

SPEKE supporta la crittografia delle chiavi di contenuto come specificato nella specifica DASH-IF CPIX con le seguenti restrizioni:

- SPEKE non supporta la verifica della firma digitale (XMLDSIG) per i payload di richiesta o risposta.
- SPEKE richiede 2048 certificati basati su RSA.

Queste restrizioni sono elencate anche in Personalizzazioni e vincoli alla specifica DASH-IF.

Implementazione della crittografia delle chiavi di contenuti

Per offrire la crittografia delle chiavi dei contenuti, includere quanto segue nelle implementazioni del provider di chiavi DRM:

- Gestire l'elemento `<cpix:DeliveryDataList>` nei payload della richiesta e della risposta.
- Fornire i valori crittografati nel `<cpix:ContentKeyList>` dei payload della risposta.

Per ulteriori informazioni su questi elementi, vedere la specifica DASH-IF CPIX 2.3.

Elemento di crittografia della chiave dei contenuti di esempio `<cpix:DeliveryDataList>` nel payload della richiesta

```
<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>
```

Elemento di crittografia della chiave dei contenuti di esempio `<cpix:DeliveryDataList>` nel payload della risposta

```
<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>
```

Elemento di crittografia della chiave dei contenuti di esempio `<cpix:ContentKeyList>` nel payload della risposta

L'esempio seguente mostra la gestione della chiave dei contenuti crittografati nell'elemento `<cpix:ContentKeyList>` del payload di risposta. Questo utilizza l'elemento `<pskc:EncryptedValue>`:

```
<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>
```

In base al confronto, l'esempio seguente mostra un payload di risposta simile con la chiave di contenuti distribuita non crittografata, come chiave in chiaro. Questo utilizza l'elemento `<pskc:PlainValue>`:

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

```
            </pskc:Secret>
        </cpix:Data>
    </cpix:ContentKey>
</cpix:ContentKeyList>
```

SPEKE API v2 - Sovrascrivere l'identificatore chiave

Il componente di crittografia crea un nuovo identificatore chiave (KID) che ruota le chiavi. Trasferisce il KID al provider di chiavi DRM nelle richieste. Quasi sempre, il provider di chiavi risponde utilizzando lo stesso KID, ma è in grado di fornire un valore diverso per il KID nella risposta.

Di seguito è riportato un esempio di richiesta con il 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>
```

La seguente risposta sovrascrive il KID in 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>
```

Licenza

Licenza pubblica internazionale Creative Commons Attribution- 4.0 ShareAlike

Esercitando i Diritti concessi in licenza (definiti di seguito), l'Utente accetta e accetta di essere vincolato dai termini e dalle condizioni della presente Licenza Pubblica Internazionale Creative Commons Attribution- ShareAlike 4.0 («Licenza pubblica»). Laddove la presente Licenza Pubblica possa essere qualificata come un contratto, Ti sono attribuiti i Diritti Concessi in Licenza a fronte della Tua accettazione di questi termini e condizioni, e il Licenziante Ti attribuisce tali diritti a fronte dei benefici che egli riceve rendendo il Materiale Concesso in Licenza disponibile secondo questi termini e condizioni.

Articolo 1 - Definizioni.

a. Materiale Elaborato significa materiale oggetto di Diritti d'Autore e Simili, che derivi o sia basato sul Materiale Concesso in Licenza nel quale il Materiale Concesso in Licenza sia tradotto, alterato, arrangiato, trasformato o altrimenti modificato, in una maniera che richieda il permesso ai sensi dei Diritti d'Autore e Simili detenuti dal Licenziante. Ai fini della presente Licenza Pubblica, laddove il Materiale Concesso in Licenza sia una composizione musicale, un'esecuzione musicale o una registrazione di suoni, la sincronizzazione del Materiale Concesso in Licenza con un'immagine in movimento costituisce sempre Materiale Elaborato.
b. Per Licenza Adattatore si intende la licenza che applichi al tuo copyright e ai tuoi diritti simili nei tuoi contributi al Materiale adattato in conformità con i termini e le condizioni della presente Licenza Pubblica.
c. Per Licenza compatibile BY-SA si intende una licenza elencata su creativecommons.org/compatiblelicenses, approvata da Creative Commons come essenzialmente equivalente della presente Licenza Pubblica.
d. Diritti d'Autore e Simili significa diritti d'autore e/o diritti simili strettamente connessi al diritto d'autore, inclusi, fra gli altri, l'esecuzione, la diffusione, la registrazione di suoni e il Diritto Sui Generis sulle Banche Dati, comunque denominati o classificati. Ai fini della presente Licenza Pubblica, i diritti specificati all'interno degli Artt. 2(b)(1)-(2) non sono Diritti d'Autore e Simili.
e. Misure Tecnologiche Efficaci significa quelle misure che, in assenza di una specifica autorizzazione, non possono essere aggirate secondo le norme che recepiscono gli obblighi previsti dall'art. 11 del Trattato OMPI sul diritto d'autore adottato il 20 dicembre 1996 e/o simili accordi internazionali.

f. Eccezioni e Limitazioni significa qualunque eccezione e/o limitazione ai Diritti D'Autore e Simili, inclusi "fair use" e "fair dealing", che si applichi al Tuo utilizzo del Materiale Concesso in Licenza.

g. Per Elementi di licenza si intendono gli attributi di licenza elencati nel nome di una licenza pubblica Creative Commons. Gli elementi di licenza di questa licenza pubblica sono Attribuzione e. ShareAlike

h. Materiale Concesso in Licenza significa qualsiasi opera artistica o letteraria, banca dati, o altro materiale al quale il Licenziante abbia applicato la presente Licenza Pubblica.

i. Diritti Concessi in Licenza significa tutti i diritti che sono concessi a Te nel rispetto dei termini e delle condizioni della presente Licenza Pubblica, limitatamente ai Diritti d'Autore e Simili che si applicano al Tuo utilizzo del Materiale Concesso in Licenza e che il Licenziante ha facoltà di licenziare.

j. Licenziante significa l'individuo, gli individui, l'ente o gli enti che concede o concedono diritti secondo la presente Licenza Pubblica.

k. Condividi/Condividere significa fornire materiale al pubblico con ogni mezzo di comunicazione o formato che richieda l'autorizzazione rispetto ai Diritti Concessi in Licenza, come la riproduzione, l'esposizione ed esecuzione in pubblico, la distribuzione, la divulgazione, la comunicazione al pubblico, l'importazione e la messa a disposizione del pubblico del materiale, anche con modalità che consentano di accedere al materiale da un luogo e in un momento scelti individualmente dal pubblico.

l. Diritto Sui Generis sulle Banche Dati significa quei diritti ulteriori rispetto al diritto d'autore individuati dalla Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996 e successive modificazioni, relativa alla tutela giuridica delle banche di dati, nonché altri diritti sostanzialmente equivalenti previsti ovunque nel mondo.

m. Tu significa l'individuo o l'ente che esercita i Diritti Concessi in Licenza secondo la presente Licenza Pubblica. Te/Tuo/Tua/Tuoi/Ti hanno un significato analogo.

Articolo 2 - Ambito di Applicazione.

a. Concessione della Licenza.

   1. Nel rispetto dei termini e delle condizioni contenute nella presente Licenza Pubblica, il Licenziante concede a Te una licenza per tutto il mondo, gratuita, non sub-licenziabile, non esclusiva e irrevocabile che Ti autorizza ad esercitare i Diritti Concessi in Licenza sul Materiale Concesso in Licenza per:

      A. riprodurre e condividere il Materiale concesso in licenza, in tutto o in parte; e

B. produrre, riprodurre e condividere materiale adattato.

2. Eccezioni e Limitazioni. Al fine di evitare dubbi, quando si applicano delle Eccezioni o Limitazioni al Tuo utilizzo, la presente Licenza Pubblica non si applica a Te e Tu non devi rispettarne i termini e le condizioni.
3. Durata. La durata della presente Licenza Pubblica è specificata all'interno dell'Art. 6(a).
4. Mezzi di comunicazione, supporti e formati; modifiche tecniche consentite. Il Licenziante Ti autorizza a esercitare i Diritti Concessi in Licenza con ogni mezzo di comunicazione, su ogni supporto e in tutti i formati esistenti e sviluppati in futuro, e ad apportare le modifiche che si rendessero tecnicamente necessarie a tale scopo. Il Licenziante rinuncia o si impegna a non far valere alcun diritto o autorità per proibire a Te di effettuare le modifiche che si rendessero tecnicamente necessarie per l'esercizio dei Diritti Concessi in Licenza, incluse le modifiche tecnicamente necessarie per aggirare Misure Tecnologiche Efficaci. Ai fini della presente Licenza Pubblica, apportare le modifiche autorizzate dal presente Art. 2(a)(4) non costituisce in alcun caso Materiale Elaborato.
5. Destinatari a valle.
   A. Offerta dal Licenziante - Materiale Concesso in Licenza. Ogni destinatario del Materiale Concesso in Licenza riceve automaticamente un'offerta dal Licenziante ad esercitare i Diritti Concessi in Licenza secondo i termini e le condizioni della presente Licenza Pubblica.
   B. Offerta aggiuntiva del Licenziante — Materiale adattato. Ogni destinatario di Materiale adattato da parte dell'Utente riceve automaticamente un'offerta dal Licenziante per esercitare i Diritti Concessi in Licenza sul Materiale adattato alle condizioni della Licenza dell'Adattatore applicata dall'Utente.
   C. Divieto di restrizioni a valle. Tu non puoi offrire o imporre termini e condizioni aggiuntive o differenti al, né applicare Misure Tecnologiche Efficaci sul, Materiale Concesso in Licenza che abbiano per effetto di restringere l'esercizio dei Diritti Concessi in Licenza da parte di qualsiasi destinatario del Materiale Concesso in Licenza.
6. Assenza di avallo. La presente Licenza Pubblica non concede né può essere interpretata in modo da concedere un'autorizzazione ad affermare o fare intendere che Tu o il Tuo utilizzo del Materiale Concesso in Licenza siate connessi, sponsorizzati, avallati o riconosciuti come ufficiali dal Licenziante o da altre parti designate a vedersi riconosciuta l'attribuzione in accordo con quanto previsto all'interno dell'Art. 3(a)(1)(A)(i).

b. Altri Diritti.

1. I diritti morali, come il diritto all'integrità, non sono oggetto della presente Licenza Pubblica, né lo sono il diritto all'immagine, il diritto alla riservatezza e/o altri simili diritti della personalità; in ogni

caso, per quanto possibile, il Licenziante rinuncia o si impegna a non far valere alcuno dei diritti sopraccitati detenuti dal Licenziante, unicamente nei limiti della misura che sia indispensabile per consentire a Te di esercitare i Diritti Concessi in Licenza.

2. I diritti su brevetti e marchi non sono oggetto della presente Licenza Pubblica.
3. Per quanto possibile, il Licenziante rinuncia al diritto esclusivo di riscuotere da Te i compensi per l'esercizio dei Diritti Concessi in Licenza, personalmente o per tramite di un ente di gestione collettiva, relativi a qualsiasi sistema di licenza volontario o rinunciabile per legge o obbligatorio. In tutti gli altri casi, il Licenziante si riserva espressamente il diritto esclusivo a riscuotere tali compensi.

Articolo 3 - Condizioni della Licenza.

Il Tuo esercizio dei Diritti Concessi in Licenza è espressamente soggetto alle seguenti condizioni.

a. Attribuzione.

1. Se Tu Condividi il Materiale Concesso in Licenza (anche in forma modificata), Tu sei tenuto a:

   A. conserva quanto segue se fornito dal Licenziante con il Materiale concesso in licenza:

```
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. indicare se l'Utente ha modificato il Materiale concesso in licenza e conservare un'indicazione di eventuali modifiche precedenti; e

   C. indica che il Materiale concesso in licenza è concesso in licenza ai sensi della presente Licenza Pubblica e includi il testo o l'URI o il collegamento ipertestuale alla presente Licenza Pubblica.

2. Tu puoi adempiere alle condizioni dell'Art. 3(a)(1) in qualsiasi maniera ragionevole, rispetto al mezzo di comunicazione, al supporto, agli strumenti e al contesto all'interno del quale Tu Condividi il Materiale Concesso in Licenza. Ad esempio, può essere ragionevole soddisfare le condizioni fornendo l'URI o il collegamento ipertestuale a una risorsa che includa le informazioni richieste.
3. Su richiesta del Licenziante, nella misura in cui ciò sia ragionevolmente praticabile, Tu devi rimuovere ognuna delle informazioni richieste dall'Art. 3(a)(1)(A).

b. ShareAlike. Oltre alle condizioni di cui alla Sezione 3 (a), se condividete materiale adattato prodotto dall'utente, si applicano anche le seguenti condizioni.
   1. La licenza dell'adattatore da applicare deve essere una licenza Creative Commons con gli stessi elementi di licenza, in questa versione o successiva, oppure una licenza compatibile con la BY-SA.
   2. È necessario includere il testo o l'URI o il collegamento ipertestuale alla licenza dell'adattatore applicata. È possibile soddisfare questa condizione in qualsiasi modo ragionevole in base al mezzo, ai mezzi e al contesto in cui condivide il Materiale adattato.
   3. L'utente non può offrire o imporre termini o condizioni aggiuntivi o diversi o applicare misure tecnologiche efficaci al Materiale adattato che limiti l'esercizio dei diritti concessi dalla Licenza dell'Adattatore applicata.

Articolo 4 - Diritto Sui Generis sulle Banche Dati.

Laddove i Diritti Concessi in Licenza dovessero includere il Diritto Sui Generis sulle Banche Dati che si applichi al Tuo utilizzo del Materiale Concesso in Licenza:

a. a scanso di equivoci, la Sezione 2 (a) (1) concede all'Utente il diritto di estrarre, riutilizzare, riprodurre e condividere tutto o una parte sostanziale del contenuto del database;
b. se includi tutto o una parte sostanziale del contenuto del database in un database in cui detieni i diritti Sui Generis sui database, allora il database su cui hai i diritti Sui Generis sul database (ma non i suoi contenuti individuali) è Materiale adattato, anche ai fini della Sezione 3 (b); e
c. Tu devi adempiere le condizioni dell'Art. 3(a) se Tu Condividi tutti i contenuti della banca dati o una loro parte sostanziale. Al fine di evitare dubbi, il presente Art. 4 si aggiunge ai, e non sostituisce i, Tuoi obblighi ai sensi della presente Licenza Pubblica, laddove i Diritti Concessi in Licenza dovessero includere Diritti d'Autore e Simili.

Articolo 5 - Esclusione di Garanzie e Limitazione di Responsabilità.

a. Laddove il Licenziante non si sia separatamente impegnato altrimenti, per quanto possibile il Licenziante offre il Materiale Concesso in Licenza "così com'è" e "come disponibile", e non fornisce alcuna dichiarazione o garanzia di qualsiasi tipo con riguardo al Materiale Concesso in Licenza, sia essa espressa o implicita, di fonte legale o di altro tipo. Questo comprende, tra le altre, le garanzie relative al titolo, alla commerciabilità, all'idoneità per un fine specifico, alla non violazione di diritti di terzi, alla mancanza di difetti latenti o di altro tipo, all'esattezza o alla presenza o assenza di errori, siano o meno conosciuti o conoscibili. Laddove l'esclusione di garanzie non sia consentita in tutto o in parte, questa esclusione può non essere applicabile a Te.

b. Per quanto possibile, il Licenziante non sarà in alcun caso responsabile nei Tuoi confronti ad alcun titolo (incluso, tra gli altri, la negligenza) o altrimenti per qualunque danno diretto, speciale, indiretto, incidentale, consequenziale, punitivo, esemplare, o altra perdita, costo, spesa o danno derivante dalla presente Licenza Pubblica o dall'utilizzo del Materiale Concesso in Licenza, anche nel caso in cui il Licenziante sia stato edotto sulla possibilità di tali perdite, costi, spese o danni. Laddove una limitazione di responsabilità non sia consentita in tutto o in parte, questa limitazione può non essere applicabile a Te.

c. L'esclusione di garanzie e la limitazione di responsabilità di cui sopra deve essere interpretata in maniera che, nei limiti consentiti dalla legge applicabile, possa avvicinarsi quanto più possibile a una esclusione totale e a uno scarico di ogni responsabilità.

Articolo 6 - Durata e Risoluzione.

a. La presente Licenza Pubblica è valida per tutta la durata dei Diritti d'Autore e Simili oggetto della presente Licenza Pubblica. Tuttavia, in caso di Tuo mancato adempimento dei termini e delle condizioni della presente Licenza Pubblica, i diritti che Ti sono concessi dalla presente Licenza Pubblica cesseranno automaticamente.

b. Quando il Tuo diritto a utilizzare il Materiale Concesso in Licenza sia cessato secondo quanto previsto dall'Art. 6(a), tale diritto è reintegrato:

   1. automaticamente a partire dalla data in cui la violazione viene sanata, a condizione che venga sanata entro 30 giorni dalla scoperta della violazione da parte dell'Utente; o
   2. previa espressa reintegrazione da parte del Licenziante.

c. Al fine di evitare dubbi, il presente Art. 6(b) non pregiudica alcun diritto di cui il Licenziante sia titolare al fine di ottenere rimedi a fronte della violazione da parte Tua della presente Licenza Pubblica.

d. Al fine di evitare dubbi, il Licenziante si riserva il diritto di rilasciare il Materiale Concesso in Licenza sulla base di termini e condizioni separati da quelli della presente Licenza Pubblica o di cessare la distribuzione del Materiale Concesso in Licenza in qualsiasi momento; in ogni caso, tali decisioni non comporteranno la risoluzione della presente Licenza Pubblica.
e. Gli Artt. 1, 5, 6, 7 e 8 rimangono validi in caso di risoluzione della presente Licenza.

Articolo 7 - Altri Termini e Condizioni.

a. Il Licenziante non sarà vincolato ad alcun altro termine o condizione aggiuntivo o differente che provenga da Te, salvo che ciò venga espressamente consentito.
b. Ogni intesa, patto o accordo aggiuntivo riguardo al Materiale Concesso in Licenza non contenuto nella presente è da considerarsi separato e indipendente dai termini e dalle condizioni della presente Licenza Pubblica.

Articolo 8 - Interpretazione.

a. Al fine di evitare dubbi, la presente Licenza Pubblica non intende, né deve essere interpretata in modo da ridurre, limitare, restringere o condizionare alcun utilizzo del Materiale Concesso in Licenza che sia lecito anche in assenza di autorizzazione ai sensi della presente Licenza Pubblica.
b. Nei limiti consentiti dalla legge applicabile, qualora una o più disposizioni della presente Licenza Pubblica siano giudicate invalide o inefficaci, saranno da intendersi rettificate nei limiti della misura che sia indispensabile per renderle valide ed efficaci. Se una o più disposizioni non possono essere rettificate, dovranno essere eliminate dalla presente Licenza Pubblica senza comportare l'invalidità o l'inefficacia dei restanti termini e condizioni.
c. In nessun caso i termini e le condizioni di cui alla presente Licenza Pubblica possono essere rinunciati né alcun mancato adempimento può essere consentito, salvo che tale rinuncia o consenso venga espressamente autorizzato dal Licenziante.
d. Nessuna parte della presente Licenza Pubblica può in alcun modo costituire o essere interpretata come una limitazione o una rinuncia a qualsiasi privilegio o immunità che possa applicarsi al Licenziante o a Te, inclusi quelli derivanti dai procedimenti giudiziari di qualsivoglia giurisdizione o autorità.

Cronologia dei documenti

La tabella seguente descrive le modifiche alla documentazione SPEKE.

SPEKE v1

Modifica	Descrizione	Data
Matrice di supporto: servizi e prodotti AWS Partner	È stata aggiunta una nuova sezione per SPEKE Support nei servizi e prodotti AWS Partner, che elenca i servizi Bitmovin.	13 gennaio 2023
Aggiornamenti per i provider della piattaforma DRM	Aggiunti collegamenti e informazioni sui nuovi partner all'elenco dei provider della piattaforma DRM.	24 gennaio 2019
Includere componenti di crittografia di terze parti	L'architettura e le descrizio ni sono state aggiornate per tenere conto dei componenti di crittografia di terze parti.	20 novembre 2018
Crittografia chiavi dei contenuti	Aggiunta l'opzione di crittogra fare le chiavi di contenuti . In precedenza, Secure Packager ed Encoder Key Exchange supportavano solo la consegna di chiavi chiare.	30 ottobre 2018
Matrice di supporto - AWS Elemental Live	Aggiunta una matrice di supporto AWS Elemental Live.	27 settembre 2018
Componenti di payload standard	Aggiunta una sezione che definisce gli elementi principali del payload JSON.	27 settembre 2018

Modifica	Descrizione	Data
Sovrascrivi KID	Aggiunto una sezione sulla sostituzione del KID da parte di un provider di chiavi.	27 settembre 2018
Link corretti al sito DASH-IF	Link corretti al sito DASH IF per la specifica CPIX e per la pagina ID di sistema.	27 settembre 2018
Copia di rilascio per AWS Elemental Live	Documentazione SPEKE aggiornata per includere i prodotti AWS Elemental.	20 luglio 2018
CMAF	Aggiornate le tabelle della matrice di supporto per i servizi per includere Common Media Application Format (CMAF).	27 giugno 2018
Rilascio iniziale	Versione iniziale di Secure Packager and Encoder Key Exchange (SPEKE) versione 1, una specifica per la comunicazione tra un crittografatore di contenuti e un fornitore di chiavi DRM. Il provider di chiavi DRM espone un'API Secure Packager e Encoder Key Exchange per gestire le richieste di chiavi in entrata.	27 Novembre 2017

SPEKE v2

Modifica	Descrizione	Data
Aggiornamenti alla sezione dei fornitori di piattaforme DRM	Aggiunti nuovi partner qualificati alla colonna SPEKE v2 dell'elenco dei fornitori di piattaforme DRM.	9 agosto 2023
Aggiornamenti alle sezioni relative agli esempi di chiamate ai metodi di lavoro Live e VOD	È stata aggiunta l'intestazione di risposta X-Speke-Version mancante nelle sezioni di esempi di chiamate al metodo di lavoro SPEKE v2 Live e VOD.	13 gennaio 2023
Aggiornamenti ai fornitori di piattaforme DRM e alla sezione relativa ai contratti di crittografia	Aggiunti nuovi partner qualificati alla colonna SPEKE v2 dell'elenco dei fornitori di piattaforme DRM. Sono stati aggiunti due nuovi esempi di contratti di crittografia e la risoluzione massima SD è stata modificata a 1024x576 in tutti gli esempi interessati.	27 gennaio 2022
Rilascio iniziale	Versione iniziale di Secure Packager and Encoder Key Exchange (SPEKE) versione 2.0, una specifica per la comunicazione tra un criptatore di contenuti e un fornitore di chiavi DRM. Il provider di chiavi DRM espone un'API Secure Packager e Encoder Key Exchange per gestire le richieste di chiavi in entrata.	7 settembre 2021

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.