Guida per partner e clienti

Specifiche per lo scambio di chiavi Secure Packager ed Encoder API

Specifiche per lo scambio di chiavi Secure Packager ed Encoder API: Guida per partner e clienti

Table of Contents

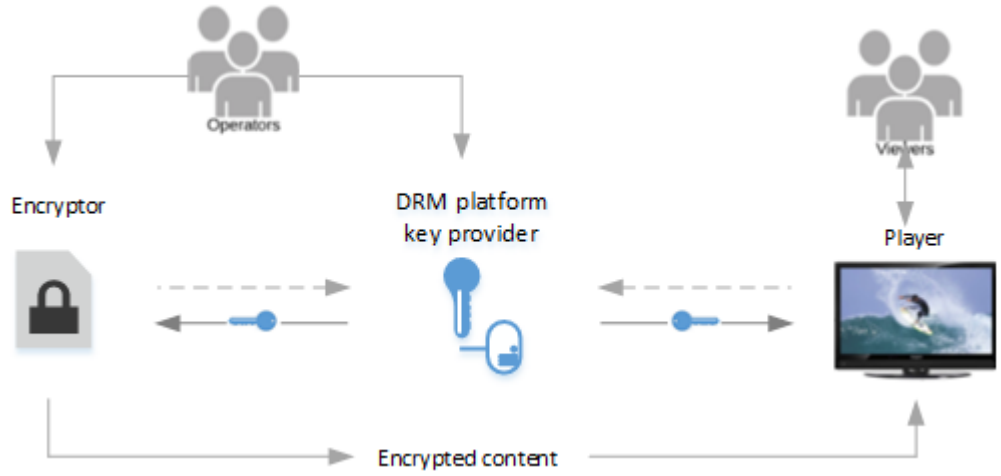
Cos'è Secure Packager and Encoder Key Exchange?

Secure Packager and Encoder Key Exchange (SPEKE) definisce lo standard per la comunicazione tra gli addetti alla crittografia e i confezionatori di contenuti multimediali e i fornitori di chiavi per la gestione dei diritti digitali (). DRM La specifica supporta i crittografi 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 SPEKE contenuti per i prodotti locali.



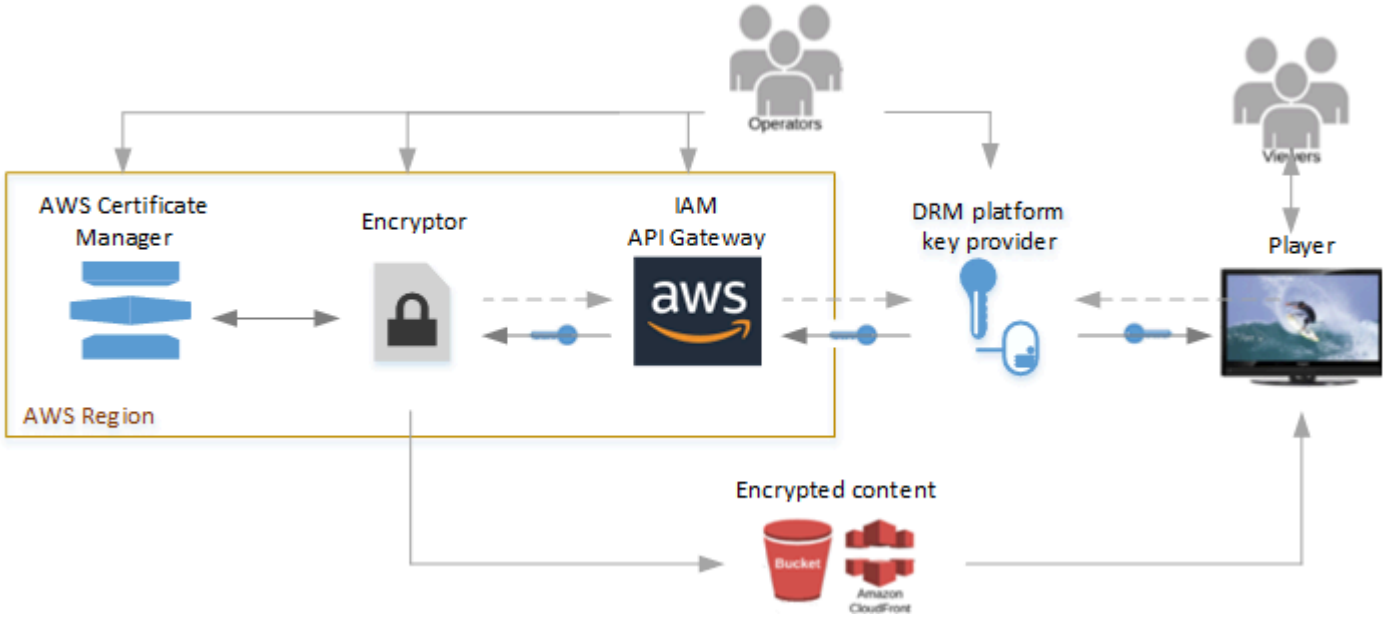
Questi sono i componenti principali dell'architettura precedente:

- Encryptor: fornisce la tecnologia di crittografia. Riceve le richieste di crittografia dal relativo operatore e recupera le chiavi richieste dal fornitore delle chiavi per proteggere il DRM contenuto crittografato.
- DRMprovider di chiavi della piattaforma: fornisce le chiavi di crittografia all'crittografo tramite un sistema -compliant. SPEKE API Il provider fornisce anche le licenze per i lettori multimediali per la decrittografia.

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

AWSarchitettura basata su cloud

La seguente illustrazione mostra l'architettura di alto livello quando SPEKE viene utilizzata con servizi e funzionalità in esecuzione nel cloud. AWS



Questi sono i principali servizi e componenti:

- Encryptor: fornisce la tecnologia di crittografia nel cloud. AWS L'encryptor riceve le richieste dal suo operatore e recupera le chiavi di crittografia richieste dal fornitore delle DRM chiavi, tramite Amazon API Gateway, per proteggere i contenuti crittografati. Fornisce i contenuti crittografati a un bucket Amazon S3 o tramite una distribuzione Amazon. CloudFront
- AWSIAMe Amazon API Gateway: gestisce i ruoli di fiducia dei clienti e le comunicazioni proxy tra l'encryptor e il fornitore di chiavi. APIGateway offre funzionalità di registrazione e consente ai clienti di controllare le loro relazioni con l'encryptor e con la piattaforma. DRM I clienti consentono l'accesso ai principali provider tramite IAM la configurazione dei ruoli. APIII gateway deve risiedere nella stessa AWS regione dell'encryptor.
- AWSCertificate Manager: (Facoltativo) 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 dei certificati deve risiedere nella stessa AWS regione del criptatore.

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

Come iniziare

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

Sei un cliente?

Collabora con un fornitore di DRM piattaforme AWS Elemental per configurare l'utilizzo della crittografia. Per i dettagli, consulta Customer Onboarding.

Sei un fornitore di DRM piattaforme o un cliente con il tuo fornitore principale?

Presentate un REST API indirizzo per il vostro fornitore principale in conformità con le SPEKE specifiche. Per i dettagli, vedere le SPEKEAPIspecifiche.

Non conosci SPEKE?

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

Per un'introduzione aSPEKE, guardate il seguente webcast:

Informazioni e specifiche relative al servizio

- APIautorizzazioni gateway: come controllare l'accesso a un API con autorizzazioni AWS Identity and Access Management (AWSIAM).
- AWS AssumeRole— Come utilizzare AWS Security Token Service (AWSSTS) per assumere la funzionalità del ruolo.
- AWSSigv4 — Come firmare una HTTP richiesta utilizzando Signature Version 4.
- DASH-IF CPIX Specification v2.0 — La versione della specifica DASH -IF Content Protection Information Exchange Format (CPIX), su cui si basa questa specifica SPEKE v1.0.
- DASH-IF CPIX Specification v2.3 — La versione della specifica DASH -IF Content Protection Information Exchange Format (CPIX), su cui si basa questa specifica v2.0. SPEKE
- DASH-Sistema IF IDs: 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 AWS account, per aiutarti a iniziare con un'SPEKEimplementazione in. AWS

Terminologia

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

- ARN— Nome della risorsa Amazon. Identifica una risorsa in modo univoco. 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 fornitore di contenuti potrebbe anche fornire file multimediali sorgente (formato mezzanino, per la transcodifica), identificatori di risorse, identificatori di chiave (KIDs), valori chiave, istruzioni di codifica e metadati di descrizione del contenuto.

- DRM— Gestione dei diritti digitali. Utilizzato per proteggere i contenuti digitali protetti da copyright da accessi non autorizzati.
- DRMpiattaforma: un sistema che fornisce DRM funzionalità e supporto ai crittografi e ai visualizzatori di contenuti, inclusa la fornitura di DRM chiavi e licenze per la crittografia e la decrittografia dei contenuti.
- DRMprovider: vedi piattaforma. DRM
- DRMsistema: uno standard per le DRM implementazioni. I DRM sistemi più comuni includono Apple FairPlay, Google Widevine e Microsoft. PlayReady DRMi sistemi vengono utilizzati dai fornitori di contenuti per proteggere i contenuti digitali per la distribuzione agli spettatori e per l'accesso da parte degli spettatori. Per un elenco dei DRM sistemi registrati con DASH -IF, vedere DASH -IF system. IDs La CPIXspecifica DASH -IF utilizza il termine "DRMsistema» come definito qui e, in alcuni punti, utilizza "DRMsistema» per indicare ciò a cui questa specifica si riferisce come piattaforma. DRM
- DRMsoluzione — Vedi DRM piattaforma.
- DRMtecnologia — Vedi DRM sistema.
- Encryptor: un componente di elaborazione multimediale che crittografa i contenuti multimediali utilizzando chiavi ottenute dal fornitore delle chiavi. I crittografi in genere aggiungono anche segnali di DRM crittografia e metadati ai supporti. I componenti di crittografia sono in genere codificatori, packager e transcoder.
- Fornitore di chiavi: il componente di una DRM piattaforma che espone a per gestire le richieste chiave. SPEKE REST API 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 DRM piattaforma 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 da diverse fonti, inclusi i file manifest multimediali, i file multimediali e DRM le licenze. Richiede licenze alla DRM piattaforma per conto degli spettatori.

Onboarding dei clienti per SPEKE

Proteggi i tuoi contenuti dall'uso non autorizzato combinando un provider di chiavi Secure Packager and Encoder Key Exchange (SPEKE) per la gestione dei diritti digitali (DRM) con il tuo sistema di crittografia e con i tuoi lettori multimediali. SPEKEdefinisce lo standard per la comunicazione tra gli addetti alla crittografia e i pacchetti di contenuti multimediali e i fornitori di chiavi per la gestione dei diritti digitali (). DRM Per effettuare l'onboarding, scegli un fornitore di chiavi DRM della piattaforma e configuri la comunicazione tra il fornitore di chiavi e i tuoi crittografi e lettori.

Argomenti

Inizia con un fornitore di piattaforme DRM

I seguenti partner Amazon forniscono implementazioni di DRM piattaforme di terze parti perSPEKE. 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.

DRMfornitore di piattaforme	SPEKEsupporto v1	SPEKEsupporto v2 (Elementa l) AWS MediaPackage
Assinoma	√	√
Acquista DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKAReti	√	√

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

SPEKEsupporto in servizi e prodotti AWS

Questa sezione elenca il SPEKE supporto fornito dai Servizi AWS multimediali eseguiti nel AWS cloud e dai prodotti multimediali AWS locali. Questi servizi e prodotti sono i crittografi dell'architettura di crittografia dei SPEKE contenuti. Verifica che il protocollo di streaming e il DRM sistema che desideri siano disponibili per il tuo servizio o prodotto.

AWSservizio o prodotto	SPEKEsupporto v1	SPEKEsupporto v2	Tecnologie supportate DRM
AWSElemental MediaConvert : servizio eseguito nel cloud AWS	√		Documentazione

AWSservizio o prodotto	SPEKEsupporto v1	SPEKEsupporto v2	Tecnologie supportate DRM
AWSElemental MediaPackage : servizio eseguito nel cloud AWS	√	√	Documentazione
AWSElemental Live - Prodotto locale	√		Documentazione: MPEG -/DASHHLS
AWSElemental Server - Prodotto locale	√		Documentazione

SPEKEassistenza nei servizi e nei prodotti dei AWS partner

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

AWSservizio o prodotto	SPEKEsupporto v1	SPEKEsupporto v2	Tecnologie supportate DRM
Codifica video live di Bitmovin	√		Documentazione
Codifica Bitmovin Video on demand () VOD	√		Documentazione

SPEKEAPIspecificazione

Questa è la REST API specifica per Secure Packager e Encoder Key Exchange ()SPEKE. Utilizzate questa specifica per fornire protezione del DRM copyright ai clienti che utilizzano la crittografia.

In un flusso di lavoro di streaming video, il motore di crittografia comunica con il fornitore di chiavi della DRM piattaforma per richiedere le chiavi di contenuto. 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:

- Definite un'interfaccia semplice, affidabile e altamente sicura che DRM fornitori e clienti possano utilizzare per l'integrazione con i sistemi di crittografia quando è richiesta la crittografia dei contenuti.
- Copri VOD e attiva i flussi di lavoro e includi le condizioni di errore e i meccanismi di autenticazione necessari per una comunicazione robusta e altamente sicura tra gli endpoint dei principali provider e gli endpoint dei principali provider. DRM
- Include il supporto e la HLS creazione MSS di DASH pacchetti e i relativi DRM sistemi comuni: FairPlay, PlayReady e Widevine/. CENC
- Mantieni le specifiche semplici ed estensibili, per supportare i DRM sistemi futuri.
- Usa un semplice RESTAPI.

> **Note**
>
>

ARISINGFROM, OUT DI O IN CONNECTION WITH THIS MATERIAL THE USE O OTHER DEALINGS DI THISMATERIAL.

Argomenti

Autenticazione richiesta per SPEKE

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

Argomenti

Autenticazione per implementazioni AWS cloud

SPEKErichiede AWS l'autenticazione tramite IAM ruoli per l'uso con un crittografo. IAMi ruoli vengono creati dal DRM provider o dall'operatore proprietario dell'DRMendpoint in un account. AWS A ogni ruolo viene assegnato un Amazon Resource Name (ARN), che l'operatore del servizio AWS Elemental fornisce sulla console di servizio quando richiede la crittografia. Le autorizzazioni relative alle policy del ruolo devono essere configurate in modo da consentire l'accesso al provider di chiavi API e nessun altro AWS accesso alle risorse. Quando il criptatore contatta il fornitore delle DRM chiavi, utilizza il ruolo ARN per assumere il ruolo di titolare dell'account del provider di chiavi, che restituisce le credenziali temporanee che il criptatore può utilizzare per accedere al fornitore delle chiavi.

Un'implementazione comune prevede che l'operatore o il fornitore della DRM piattaforma utilizzi Amazon API Gateway davanti al provider principale e quindi abiliti l'autorizzazione AWS Identity and Access Management (AWSIAM) 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 riguardano 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 ruolo ARN creato per accedere al provider di DRM chiavi:

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

Per ulteriori informazioni sulla creazione di un ruolo, vedere AWS AssumeRole. Per ulteriori informazioni sulla firma di una richiesta, vedere AWSSigv4.

Autenticazione per prodotti locali

Per i prodotti locali, si consiglia di utilizzare l'autenticazioneSSL/TLSe digest per la massima sicurezza, ma come minimo è consigliabile utilizzare l'autenticazione di base su. HTTPS

Entrambi i tipi di autenticazione utilizzano l'`Authorization`intestazione 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 MD5 hash che includono un one-time-use nonce univoco proveniente dal server che viene 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 sull'autenticazione di base e digest, incluse informazioni dettagliate sull'intestazione, consultate la specifica RFC2617 della Internet Engineering Task Force (IETF) - HTTP Authentication: Basic and Digest Access Authentication.

SPEKEAPIv1

Questa è la versione 1 REST API di Secure Packager e Encoder Key Exchange ()SPEKE. Utilizzate questa specifica per fornire protezione del DRM copyright ai clienti che utilizzano la crittografia. Per essere SPEKE conforme, il fornitore delle DRM chiavi deve esporre quanto REST API descritto in questa specifica. L'encryptor effettua API chiamate al fornitore delle chiavi.

> **Note**
>
> Il codice di esempio in questa specifica è soltanto indicativo. Non puoi eseguire gli esempi perché non fanno parte di un'implementazione completaSPEKE.

SPEKEutilizza la definizione della struttura dei dati DASH dell'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 DRM scambio multiplo estensibile dalla DRM piattaforma al criptatore. 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 packaging con bitrate adattivo includono, e. HLS DASH MSS

Per informazioni dettagliate sul formato di scambio, consultate le CPIX specifiche dell'DASHIndustry Forum all'indirizzo https://dashif.org/docs/ DASH -IF- -v2-0.pdf. CPIX

Argomenti

- SPEKEAPIv1 - Personalizzazioni e vincoli alla specifica -IF DASH
- SPEKEAPIv1 - Componenti del payload standard
- SPEKEAPIv1 - Esempi di chiamate al metodo Live Workflow
- SPEKEAPIv1 - esempi di chiamata al metodo VOD di lavoro
- SPEKEAPIv1 - Crittografia con chiave del contenuto
- SPEKEAPIv1 - Battito cardiaco
- SPEKEAPIv1 - Sovrascrivere l'identificatore della chiave

SPEKEAPIv1 - Personalizzazioni e vincoli alla specifica -IF DASH

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

- SPEKE segue il flusso di lavoro Encryptor Consumer.
- Per le chiavi di contenuto crittografato, SPEKE applica le seguenti restrizioni:
  - SPEKEnon supporta la verifica della firma digitale (XMLDSIG) per i payload di richiesta o risposta.
  - SPEKErichiede certificati RSA basati su 2048.
- Per i flussi di lavoro chiave a rotazione, SPEKE richiede il `ContentKeyUsageRule` filtro,. `KeyPeriodFilter` SPEKEignora tutte le altre impostazioni. `ContentKeyUsageRule`
- SPEKE omette la funzionalità `UpdateHistoryItemList`. Se l'elenco è presente nella risposta, lo SPEKE ignora.
- SPEKEsupporta la rotazione dei tasti. SPEKEutilizza 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 quanto riguarda il HLS packaging, se `URIExtXKey` è presente nella risposta, deve contenere i dati completi da aggiungere nel URI parametro del `EXT-X-KEY` tag di una HLS playlist, senza ulteriori requisiti di segnalazione.
- Per la HLS playlist, sotto il `DRMSystem` tag, SPEKE fornisce i parametri personalizzati opzionali `speke:KeyFormat` `espeke:KeyFormatVersions`, per i valori `KEYFORMAT` e i `KEYFORMATVERSIONS` parametri del `EXT-X-KEY` tag.

  Il vettore di HLS inizializzazione (IV) segue sempre il numero del segmento, a meno che non sia specificato esplicitamente 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.
- SPEKEattualmente non supporta più tracce o chiavi per contenuto.

  L'encryptor SPEKE -compliant funge da client e invia `POST` le operazioni all'endpoint del provider chiave. 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.

SPEKEAPIv1 - Componenti del payload standard

In qualsiasi SPEKE richiesta, l'encryptor può richiedere risposte per uno o più sistemi. DRM L'encryptor specifica i DRM sistemi inclusi nel `<cpix:DRMSystemList>` payload della richiesta. Ogni specifica di sistema include la chiave e indica il tipo di risposta da restituire.

L'esempio seguente mostra un elenco di sistemi con un'unica specifica di DRM 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 DRM sistema, registrato presso l'organizzazione DASH IF. Per un elenco, vedere DASH-IF System. IDs
`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 un'intestazione specifica per il sistema di protezione ()PSSH. Questo tipo di intestazi one contiene un riferimento ai`kid`, oltre ai dati personalizzati per il DRM fornitore`systemID`, 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 dall'encryptor al fornitore di DRM chiavi, con i componenti principali evidenziati. La prima richiesta riguarda una chiave standard, mentre la seconda richiede una PSSH risposta:

```
<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 del fornitore di DRM chiavi all'encryptor:

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

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

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

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

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

SPEKEAPIv1 - Esempi di chiamate al metodo Live Workflow

Richiedi esempio di sintassi

Quanto segue URL è un esempio e non indica un formato fisso:

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

Corpo della richiesta

Un CPIX elemento.

Intestazioni di richiesta

Nome	Tipo	Si verifica	Descrizione
`AWS Authorization`	Stringa	1..1	Vedi AWSSigv4
`X-Amz-Security-Token`	Stringa	1..1	Vedi Sigv4 AWS
`X-Amz-Date`	Stringa	1..1	Vedi Sigv4 AWS
`Content-Type`	Stringa	1..1	application/xml

Intestazioni di risposta

Nome	Tipo	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

HTTP CODE	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	DASH- risposta del payload 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, vedere Content Key encryption.

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 DRM provider di chiavi:

```
<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

L'esempio seguente mostra un payload di risposta tipico del 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>
```

SPEKEAPIv1 - esempi di chiamata al metodo VOD di lavoro

Richiedi esempio di sintassi

Quanto segue URL è un esempio e non indica un formato fisso.

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

Corpo della richiesta

Un CPIX elemento.

Intestazioni di risposta

Nome	Tipo	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

HTTP CODE	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	DASH- risposta CPIX del carico utile
`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, vedere Content Key encryption.

VODEsempio: Request Payload with Keys in the Clear

L'esempio seguente mostra un payload di VOD richieste di base dall'encryptor 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>
```

VODEsempio: Response Payload with Keys in the Clear

L'esempio seguente mostra un payload di VOD risposta di base fornito dal fornitore di DRM chiavi:

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

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

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

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

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

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

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

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

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

SPEKEAPIv1 - Crittografia con chiave del contenuto

Facoltativamente, puoi aggiungere la crittografia con chiave di contenuto alla tua SPEKE implementazione. 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 con chiave di contenuto per i crittografi in esecuzione nel AWS Cloud, i clienti importano i certificati nel AWS Certificate Manager e quindi utilizzano il certificato risultante ARNs per le loro attività di crittografia. L'encryptor utilizza il certificato ARNs e il ACM servizio per fornire chiavi di contenuto crittografate al fornitore delle chiavi. DRM

Restrizioni

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

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

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

Implementazione della crittografia delle chiavi di contenuti

Per fornire la crittografia delle chiavi di contenuto, includi 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 2.0.

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>
```

SPEKEAPIv1 - Battito cardiaco

Richiedi esempio di sintassi

Quanto segue URL è un esempio e non indica un formato fisso:

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

Richiesta e risposta

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

SPEKEAPIv1 - Sovrascrivere l'identificatore della chiave

L'encryptor crea un nuovo identificatore di chiave (KID) ogni volta che ruota le chiavi. Lo passa KID al fornitore delle DRM chiavi nelle sue richieste. Quasi sempre, il fornitore di chiavi risponde utilizzando lo stesso metodoKID, ma può fornire un valore diverso KID nella risposta.

Di seguito è riportato un esempio di richiesta con: 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 risposta seguente sostituisce la KID risposta a: `22222222-2222-2222-2222-222222222222`

```
    <cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
     <cpix:ContentKeyList>
      <cpix:ContentKey explicitIV="ASgwx9pQ2/2lnDzJsUxWcQ=="
kid="22222222-2222-2222-2222-222222222222">
       <cpix:Data>
        <pskc:Secret>
         <pskc:PlainValue>p3dWaHARtL97MpT7TE916w==</pskc:PlainValue>
        </pskc:Secret>
       </cpix:Data>
      </cpix:ContentKey>
     </cpix:ContentKeyList>
     <cpix:DRMSystemList>
      <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
```

```
        <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOY
cpix:PSSH>
       </cpix:DRMSystem>
      </cpix:DRMSystemList>
      <cpix:ContentKeyPeriodList>
       <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
      </cpix:ContentKeyPeriodList>
      <cpix:ContentKeyUsageRuleList>
       <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222">
        <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
       </cpix:ContentKeyUsageRule>
      </cpix:ContentKeyUsageRuleList>
     </cpix:CPIX>
```

SPEKEAPIv2

Questa è la versione 2 REST API di Secure Packager e Encoder Key Exchange ()SPEKE. Utilizzate questa specifica per fornire protezione del DRM copyright ai clienti che utilizzano la crittografia. Per essere SPEKE conforme, il fornitore delle DRM chiavi deve esporre quanto REST API descritto in questa specifica. L'encryptor effettua API chiamate al fornitore delle chiavi.

> **Note**
>
> Il codice di esempio in questa specifica è soltanto indicativo. Non puoi eseguire gli esempi perché non fanno parte di un'implementazione completaSPEKE.

SPEKEutilizza la definizione della struttura dei dati DASH dell'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 DRM scambio multiplo estensibile dalla DRM piattaforma al criptatore. 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 packaging con bitrate adattivo includono, e. HLS DASH MSS

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

Sul SPEKE lato, questo viene applicato attraverso l'uso dell'`X-Speke-Version`HTTPintestazione e sul CPIX lato attraverso l'uso dell'attributo. `CPIX@version` La mancanza di questi elementi nelle richieste è tipica dei flussi di lavoro precedenti della SPEKE versione 1. Nei flussi di lavoro SPEKE v2, il fornitore delle chiavi dovrebbe elaborare CPIX i documenti solo se supporta entrambi i parametri di versione.

Per informazioni dettagliate sul formato di scambio, consultate le specifiche dell'DASHIndustry Forum CPIX2.3.

Nel complesso, la SPEKE versione 2.0 presenta le seguenti evoluzioni rispetto alla SPEKE versione 1.0:

- Tutti i tag del SPEKE XML namespace sono obsoleti a favore di tag equivalenti nel namespace CPIX XML
- `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 CPIX attributi obbligatori:`CPIX@version`, `ContentKey@commonEncryptionScheme`
- Nuovo CPIX elemento opzionale: `DRMSystem.ContentProtectionData`
- Support per più chiavi di contenuto
- Meccanismo di controllo incrociato tra e SPEKE CPIX
- HTTPevoluzione delle intestazioni: nuova intestazione, `X-Speke-Version` intestazione rinominata in `Speke-User-Agent` `X-Speke-User-Agent`
- APIdeprecazione del battito cardiaco

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

Argomenti

- SPEKEAPIv2 - Personalizzazioni e vincoli alla specifica -IF DASH
- SPEKEAPIv2 - Componenti del payload standard
- SPEKEAPIv2 - Contratto di crittografia
- SPEKEAPIv2 - Esempi di chiamate al metodo Live Workflow

- SPEKEAPIv2 - VOD esempi di chiamata al metodo di lavoro
- SPEKEAPIv2 - Crittografia delle chiavi del contenuto
- SPEKEAPIv2 - Sovrascrivere l'identificatore chiave

SPEKEAPIv2 - Personalizzazioni e vincoli alla specifica -IF DASH

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

CPIXProfilo

- SPEKE segue il flusso di lavoro Encryptor Consumer.
- Per le chiavi di contenuto crittografate, SPEKE applica le seguenti restrizioni:
  - SPEKEnon supporta la verifica della firma digitale (XMLDSIG) per i payload di richiesta o risposta.
  - SPEKErichiede certificati RSA basati su 2048.
- SPEKEsfrutta solo un sottoinsieme di funzionalità: CPIX
  - SPEKE omette la funzionalità `UpdateHistoryItemList`. Se l'elenco è presente nella risposta, SPEKE lo ignora.
  - SPEKEomette la funzionalità dei tasti root/leaf. Se l'`ContentKey@dependsOnKey`attributo è presente nella risposta, lo ignora. SPEKE
  - SPEKEomette l'`BitrateFilter`elemento e l'`VideoFilter@wcg`attributo. Se questi elementi o attributi sono presenti nel CPIX payload, lo SPEKE 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 CPIX documenti scambiati con la v2. SPEKE
- Se inclusi in una CPIX richiesta dell'encryptor, tutti gli elementi e gli attributi devono riportare un valore valido nella risposta del fornitore di chiavi. CPIX In caso contrario, l'encryptor si fermerà e genererà un errore.
- SPEKEsupporta la rotazione dei tasti con `KeyPeriodFilter` elementi. SPEKEutilizza solo il `ContentKeyPeriod@index` per tenere traccia del periodo chiave.

- Per la HLS segnalazione, 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 della chiave.

  `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 @version 'CPIX. Quando si riceve una richiesta con una versione non supportata, la descrizione dell'errore restituita dal fornitore della chiave è «CPIXUnsupported @version».

  `CPIX@version`il valore non può essere sovrascritto dal fornitore di chiavi.
- 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 CPIX documento unico non può combinare più valori per `ContentKey@commonEncryptionScheme` attributi diversi. 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 DRMSystem`id`».

  `ContentKey@commonEncryptionScheme`il valore non può essere sovrascritto dal fornitore della chiave.

- Quando riceve valori diversi per `DRMSystem@PSSH` XML `<pssh>` un elemento `DRMSystem.ContentProtectionData` interno nel corpo della CPIX risposta, il criptatore si ferma e genera un errore.

API per CPIX

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

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

  Se il fornitore della chiave non restituisce un errore ma non riesce a restituire un CPIX documento che include le informazioni obbligatorie, l'encryptor dovrebbe interrompersi 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 HTTP risposta 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@ non contentId è definito	CPIX@ mancante contentId
CPIX@version non è definito	Manca CPIX @version
CPIX@version non è supportato	@version non supportato CPIX

Caso di errore	Messaggio di errore
ContentKey@ non commonEncryptionScheme è definito	ContentKey@ mancante commonEncryptionScheme per KID `id` (dove è `id` uguale al valore ContentKey @kid)
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 supportata SPEKE	Versione non SPEKE supportata
Il contratto di crittografia non è valido	Contratto di crittografia non valido
Il contratto di crittografia contraddice i vincoli relativi ai livelli DRM di sicurezza	Il contratto di CPIX crittografia richiesto non è supportato
Il contratto di crittografia non include alcun AudioFilter elemento VideoFilter or	Contratto CPIX di crittografia mancante

SPEKEAPIv2 - Componenti del payload standard

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

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

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

Questa è una sezione obbligatoria, rilevante sia per il live che per VOD lo streaming, 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 le CPIX specifiche, i possibili valori dell'`ContentKey@commonEncryptionSchemeattributo` sono definiti nella specifica Common encryption in ISO base media file format files (ISO/IEC23001-7:2016):

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

L'esempio seguente mostra un CPIX documento 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 : >DRMSystemListContentKeyUsageRuleList	uno<cpix : >, uno <cpix : >DeliveryDataListContentKey PeriodList
<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

Sezione <cpix : >DRMSystemList

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

L'esempio seguente mostra un elenco DRM di sistemi con un'unica specifica di PlayReady DRM sistema:

```
<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 di DRMsystemIDs, consulta la sezione Protezione dei contenuti del repository DASH -IF Identifiers.

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

`DRMSystem@PSSH`è obbligatorio se ISO - l'BMFFincapsulamento viene applicato ai segmenti multimediali. `DRMSystem.ContentProtectionData`XML`<pssh>`l'elemento interno viene sfruttato dal criptatore solo per scopi di segnalazione manifesta.

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

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

Sezione <cpix : >ContentKeyPeriodList

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'utilizzo UUIDs 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 si utilizzano periodi crittografici, le chiavi di crittografia devono essere allegate anche a uno dei periodi crittografici del CPIX documento, come mostrato nella sezione seguente.

Sezione <cpix : >ContentKeyUsageRuleList

Questa è una sezione obbligatoria, rilevante sia per il live che per VOD lo streaming, 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	periodId	-	-	-

Elemento supportato da SPEKE	Attributi obbligatori	Attributi facoltativi	Elementi secondari obbligatori	Elementi secondari opzionali
<cpix : >AudioFilter	-	minChannels, maxChannels	-	-
<cpix : >VideoFilter	-	minPixels, leimaxPixels, 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.

–

SPEKEAPIv2 - 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 CPIX documento 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 CPIX documento. 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@intendedTrackTypeattributo.

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@intendedTrackTypeattributo. 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@intendedTrackTypeattributo 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

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

CPIXtipo di filtro	SPEKESupporto generale	Attributi di filtro supportati da SPEKE	Attributi di filtro non supportati da SPEKE
<cpix : >VideoFilter	Sì	minPixels, hdrmaxPixels, (attributi opzionali minFps) maxFps	wcg

CPIXtipo di filtro	SPEKESupporto generale	Attributi di filtro supportati da SPEKE	Attributi di filtro non supportati da SPEKE
<cpix : >AudioFilter	Sì	minChannels, maxChannels (attributi opzionali)	
<cpix : >KeyPeriodFilter	Sì	periodId (attributo obbligatorio)	
<cpix : >BitrateFilter	No	N/D	N/D
<cpix : >LabelFilter	No	N/D	N/D

Secondo le CPIX specifiche di VideoFilter, [minPixels,maxPixels] è un intervallo completo in entrambe le dimensioni, mentre (minFps,maxFps] è incluso solo per la dimensione. maxFps Perché 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)	L'encryptor dovrebbe esaminare la sua configurazione (esterna al CPIX payload) e verificare che le tracce interessate non richiedano la crittografia. Se non è l'aspettativa, l'encryptor dovrebbe generare un errore e interrompere l'elaborazione.	Non rilevante: il fornitore delle chiavi non conosce la struttura dello streamset.

In questa situazione	Il criptatore dovrebbe/deve...	Il fornitore delle chiavi dovrebbe/deve...
Diverse regole si sovrappon gono e suggeriscono più chiavi di contenuto per crittografare una traccia specifica	Il criptatore deve applicare l'ultima valuta valutata ContentKeyUsageRule con successo nell'ordine del documento.	Non pertinente: il fornitore di chiavi non conosce la struttura dello streamset.
Il contratto di crittografia cambia in un singolo ciclo di SPEKE richiesta/risposta	L'encryptor 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 della chiave non deve modificar e un contratto di crittografia ricevuto nel CPIX payload 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 SPEKE richiesta al fornitore della chiave, poiché molto probabilmente provocherebbe una protezion e errata dei contenuti o lascerebbe alcune tracce non protette.	Il fornitore della chiave deve sollevare un'eccezione e restituire un errore relativo al «contratto di crittografia non valido».

In questa situazione	Il criptatore dovrebbe/deve...	Il fornitore delle chiavi dovrebbe/deve...
Contratto di crittografia ben strutturato, ma che viola i vincoli dei livelli di DRM sicurezza: 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 DRM sicurezza, dovrebbe sollevare un'eccezi one, interrompere l'elabora zione e non inviare la SPEKE richiesta al fornitore delle chiavi, poiché molto probabilm ente comporterebbe una protezione errata dei contenuti .	Il fornitore della chiave deve sollevare un'eccezione e restituire l'errore «Contratto di crittografia richiesto non supportato»CPIX.
Contratto di crittografia mancante	Il criptatore non deve inviare CPIX documenti che non contengano alcun elemento VideoFilter or AudioFilter .	Il fornitore della chiave deve sollevare un'eccezione e restituire l'errore «Contratto di CPIX crittografia 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///HD1HD2UHD1/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>
```

SPEKEAPIv2 - Esempi di chiamate al metodo Live Workflow

Richiedi esempio di sintassi

Quanto segue URL è un esempio e non indica un formato fisso:

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

Corpo della richiesta

Un CPIX documento.

Intestazioni di richiesta

Nome	Tipo	Si verifica	Descrizione
`AWS Authorization`	Stringa	1..1	Vedi AWSSigv4

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

Intestazioni di risposta

Nome	Tipo	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	SPEKEAPIversione utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, come '2.0' per SPEKE v2.0

Richiesta e risposta

HTTP CODE	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	DASH- risposta del CPIX payload
`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, vedere Content Key encryption.

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, con una DRM 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 del fornitore di DRM chiavi (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>
```

SPEKEAPIv2 - VOD esempi di chiamata al metodo di lavoro

Richiedi esempio di sintassi

Quanto segue URL è un esempio e non indica un formato fisso.

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

Corpo della richiesta

Un CPIX documento.

Intestazioni di richiesta

Nome	Tipo	Si verifica	Descrizione
`AWS Authorization`	Stringa	1..1	Vedi AWSSigv4
`X-Amz-Security-Token`	Stringa	1..1	Vedi Sigv4 AWS
`X-Amz-Date`	Stringa	1..1	Vedi Sigv4 AWS

Nome	Tipo	Si verifica	Descrizione
`Content-Type`	Stringa	1..1	application/xml
`X-Speke-Version`	Stringa	1..1	SPEKEAPIversione utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, come '2.0' per SPEKE v2.0

Intestazioni di risposta

Nome	Tipo	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	SPEKEAPIversione utilizzata con la richiesta, formulata come. MajorVersion MinorVersion, come '2.0' per SPEKE v2.0

Richiesta e risposta

HTTP CODE	Nome payload	Si verifica	Descrizione
`200 (Success)`	CPIX	1..1	DASH- risposta del CPIX payload
`4XX (Client error)`	Messaggio di errore del client	1..1	Descrizione dell'errore del client

HTTP CODE	Nome payload	Si verifica	Descrizione
`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, vedere Content Key encryption.

VODEsempio: Request Payload with Keys in the Clear

L'esempio seguente mostra un tipico payload di VOD richiesta dall'encryptor al provider di chiavi, con una DRM 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>
```

VODEsempio di payload di risposta con Keys in the Clear

L'esempio seguente mostra un tipico payload di risposta fornito dal fornitore di DRM chiavi (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>
```

SPEKEAPIv2 - Crittografia delle chiavi del contenuto

Facoltativamente, puoi aggiungere la crittografia con chiave di contenuto alla tua SPEKE implementazione. 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 con chiave di contenuto per i crittografi in esecuzione nel AWS Cloud, i clienti importano i certificati nel AWS Certificate Manager e quindi utilizzano il certificato risultante ARNs per le loro attività di crittografia. L'encryptor utilizza il certificato ARNs e il ACM servizio per fornire chiavi di contenuto crittografate al fornitore delle chiavi. DRM

Restrizioni

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

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

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

Implementazione della crittografia delle chiavi di contenuti

Per fornire la crittografia delle chiavi di contenuto, includi 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>
```

SPEKEAPIv2 - Sovrascrivere l'identificatore chiave

L'encryptor crea un nuovo identificatore di chiave (KID) ogni volta che ruota le chiavi. Lo passa KID al fornitore delle DRM chiavi nelle sue richieste. Quasi sempre, il fornitore di chiavi risponde utilizzando lo stesso metodoKID, ma può fornire un valore diverso KID nella risposta.

Di seguito è riportato un esempio di richiesta con: 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 risposta seguente sostituisce la KID risposta a: 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 per la specifica SPEKE API

Licenza pubblica internazionale Creative Commons Attribution- ShareAlike 4.0

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. Per misure tecnologiche efficaci si intendono quelle misure che, in assenza di un'autorità adeguata, non possono essere aggirate ai sensi delle leggi che soddisfano gli obblighi ai sensi dell'articolo 11 del Trattato sul diritto d'autore adottato il 20 dicembre 1996 e/o di accordi internazionali simili. WIPO

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 il collegamento ipertestuale alla URI 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 un collegamento ipertestuale URI o un collegamento ipertestuale a una risorsa che include 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 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 al Materiale adattato, né applicare misure tecnologiche efficaci al Materiale adattato che limiti l'esercizio dei diritti concessi dalla Licenza dell'Adattatore applicata dall'utente.

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 per la guida per SPEKE partner e clienti

La tabella seguente descrive le modifiche alla SPEKE documentazione.

SPEKE v1

Modifica	Descrizione	Data
Matrice di supporto: servizi e prodotti dei AWS partner	È stata aggiunta una nuova sezione per l'SPEKEas sistenza nei servizi e prodotti dei AWS partner, che elenca i servizi Bitmovin.	13 gennaio 2023
Aggiornamenti ai fornitori di piattaforme DRM	Aggiunti link e nuove informazi oni sui partner all'elenco dei fornitori di DRM piattaforme.	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 con chiavi trasparenti.	30 ottobre 2018
Matrice di supporto - AWS Elemental Live	Aggiunta una AWS matrice di supporto Elemental Live.	27 settembre 2018

Modifica	Descrizione	Data
Componenti di payload standard	È stata aggiunta una sezione che definisce gli elementi principali del JSON payload.	27 settembre 2018
KIDsovrascrivere	È stata aggiunta una sezione sulle KID sostituzioni da parte di un fornitore chiave.	27 settembre 2018
Collegamenti corretti al sito -IF DASH	Collegamenti corretti al sito DASH IF per le CPIX specifich e e per la pagina di sistema. IDs	27 settembre 2018
Copia di rilascio per AWS Elemental Live	È stata aggiornata la SPEKE documentazione per includere i prodotti AWS Elemental.	20 luglio 2018
CMAF	Sono state aggiornate le tabelle delle matrici di supporto per i servizi in modo da includere il Common Media Application Format (CMAF).	27 giugno 2018
Rilascio iniziale	Versione iniziale di Secure Packager e Encoder Key Exchange (SPEKE) versione 1, una specifica per la comunicazione tra un crittogra fo dei contenuti e un fornitore di chiavi. DRM Il provider di DRM chiavi utilizza Secure Packager e Encoder Key Exchange per gestire le richieste di chiavi in entrata. API	27 Novembre 2017

SPEKE v2

Modifica	Descrizione	Data
Aggiornamenti alla sezione dedicata ai fornitori di piattaforme DRM	Aggiunti nuovi partner qualificati alla colonna SPEKE v2 dell'elenco dei fornitori di DRM piattaforme.	9 agosto 2023
Aggiornamenti alle sezioni relative agli esempi di chiamate ai metodi Live e VOD Workflow	È stata aggiunta l'intestazione di risposta X-Speke-Version mancante nelle sezioni relative agli esempi di chiamate ai metodi di lavoro di SPEKE v2 Live e VOD Workflow.	13 gennaio 2023
Aggiornamenti ai fornitori di piattaforme e alla sezione relativa ai contratti di crittografia DRM	Aggiunti nuovi partner qualificati alla colonna SPEKE v2 dell'elenco dei fornitori di DRM piattaforme. 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 e Encoder Key Exchange (SPEKE) versione 2.0, una specifica per la comunicazione tra un crittografo dei contenuti e un fornitore di chiavi. DRM Il provider di DRM chiavi utilizza Secure Packager e Encoder Key Exchange per gestire le richieste di chiavi in entrata. API	7 settembre 2021

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.