Guía para socios y clientes

Especificación de API de Secure Packager and Encoder Key Exchange

Especificación de API de Secure Packager and Encoder Key Exchange: Guía para socios y clientes

Table of Contents

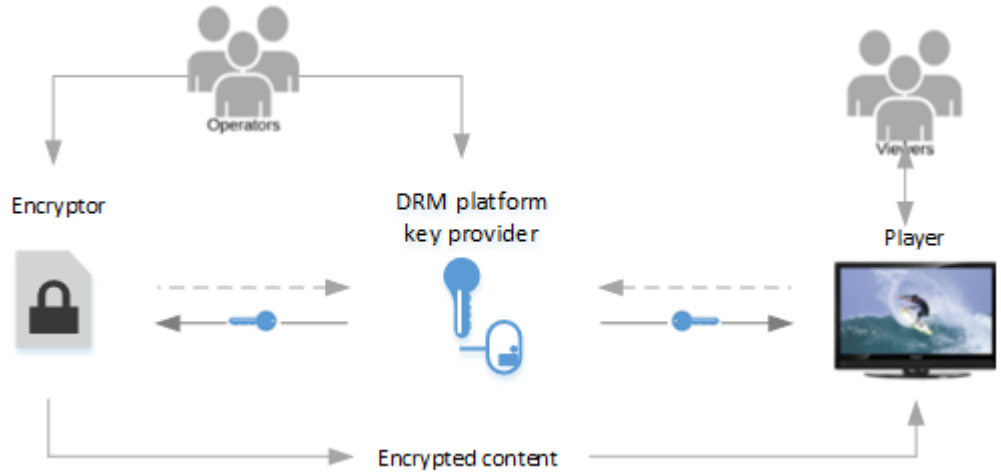
¿Qué es Secure Packager and Encoder Key Exchange?

Secure Packager and Encoder Key Exchange (SPEKE) define el estándar para la comunicación entre los encriptadores y los empaquetadores de contenido multimedia y proveedores de claves de administración de derechos digitales (DRM). La especificación se adapta a los cifradores que se ejecutan en las instalaciones y en la nube de AWS.

Temas

Arquitectura general

En la siguiente ilustración, se muestra una vista general de la arquitectura de cifrado de contenido de SPEKE para productos en las instalaciones.



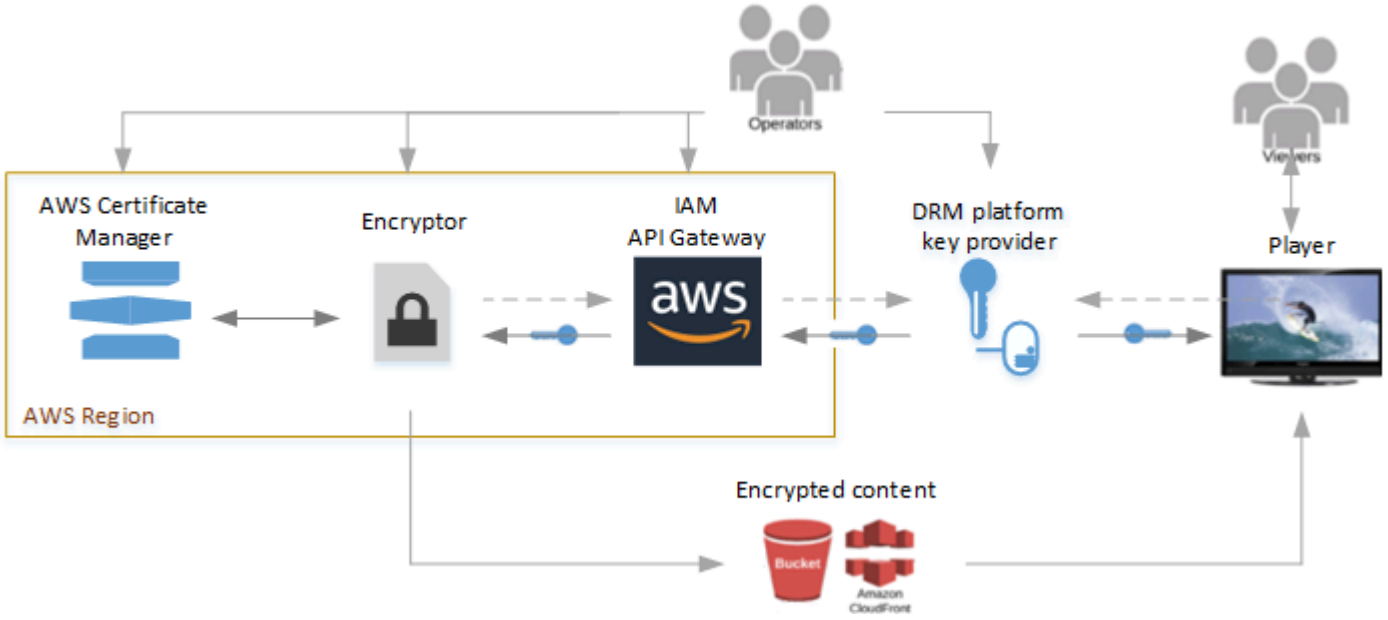
Estos son los principales componentes de la arquitectura anterior:

- Encriptador: proporciona la tecnología de cifrado. Recibe las solicitudes de cifrado del operador y recupera las claves pertinentes del proveedor de claves de DRM para proteger el contenido cifrado.
- Proveedor de claves de plataforma DRM: proporciona claves de cifrado al encriptador a través de una API compatible con SPEKE. El proveedor también proporciona licencias a los reproductores multimedia para que puedan descifrar el contenido.

- Reproductor: solicita las claves del mismo proveedor de claves de la plataforma DRM, que utiliza para desbloquear el contenido y proporcionárselo a sus usuarios.

Arquitectura basada en la nube de AWS

En la siguiente ilustración se muestra la arquitectura de alto nivel cuando SPEKE se utiliza con servicios y características que se ejecutan en la nube de AWS.



Estos son los principales servicios y componentes:

- Encriptador: proporciona la tecnología de cifrado en la nube de AWS. El encriptador recibe las solicitudes de su operador y recupera las claves de cifrado necesarias del proveedor de claves DRM, a través de Amazon API Gateway, para proteger el contenido cifrado. Entrega el contenido cifrado a un bucket de Amazon S3 o a través de una CloudFront distribución de Amazon.
- AWS IAM y Amazon API Gateway: administra las funciones de confianza del cliente y la comunicación proxy entre el encriptador y el proveedor de claves. API Gateway dispone de funcionalidades de registro y permite a los clientes controlar sus relaciones con el encriptador y con la plataforma DRM. Los clientes habilitan el acceso al servidor de claves a través de la configuración de roles de IAM. API Gateway debe residir en la misma región de AWS que el cifrador.
- AWS Certificate Manager: (opcional) proporciona administración de certificados para el cifrado de claves de contenido. El cifrado de claves de contenido es una práctica recomendada para proteger

la comunicación. El administrador de certificados debe estar en la misma región de AWS que el encriptador.

- Proveedor de claves de plataforma DRM: proporciona claves de cifrado al encriptador a través de una API compatible con SPEKE. El proveedor también proporciona licencias a los reproductores multimedia para que puedan descifrar el contenido.
- Reproductor: solicita las claves del mismo proveedor de claves de la plataforma DRM que utiliza para desbloquear el contenido y proporcionárselo a sus usuarios.

Cómo comenzar

Para obtener material introductorio adicional sobre SPEKE, consulte ¿Es la primera vez que utiliza SPEKE?.

¿Es cliente?

Asóciese con el proveedor de plataforma DRM de AWS Elemental para usar el cifrado. Para obtener más información, consulte Incorporación de clientes.

¿Es usted un proveedor de plataforma DRM o un cliente con su propio proveedor de claves?

Exponga una API de REST para su proveedor de claves de conformidad con la especificación de SPEKE. Para obtener más información, consulte la especificación de la API de SPEKE.

¿Es la primera vez que utiliza SPEKE?

En esta sección se proporciona información introductoria para los lectores que no conocen Secure Packager y Encoder Key Exchange (SPEKE).

Para obtener una introducción a SPEKE, vea el siguiente webcast:

Información y especificaciones de servicio relacionadas

- Permisos a puertas de enlace de API: cómo controlar el acceso a una API con permisos de AWS Identity and Access Management (AWS IAM).
- AWS AssumeRole: cómo utilizar el Servicio de Token de Seguridad de AWS (AWS STS) para asumir la funcionalidad del rol.
- AWS Sigv4: cómo firmar una solicitud HTTP con Signature Versión 4.
- Especificación v2.0 de DASH-IF CPIX: versión de la especificación del formato de intercambio de información de protección de contenido (CPIX) de DASH-IF, en la que se basa la especificación SPEKE v1.0.
- Especificación v2.3 de DASH-IF CPIX: versión de la especificación del formato de intercambio de información de protección de contenido (CPIX) de DASH-IF, en la que se basa la especificación SPEKE v2.0.
- Sistema DASH-IF IDs: lista de identificadores registrados para los sistemas DRM.
- https://github.com/awslabs/speke-reference-server— Ejemplo de proveedor de claves de referencia que puede utilizar con su cuenta de AWS para ayudarle a empezar con una implementación de SPEKE en AWS.

Terminología

La siguiente lista define la terminología utilizada en esta especificación. Siempre que sea posible, esta especificación sigue la terminología utilizada en la especificación DASH-IF CPIX.

- ARN: nombre de recurso de Amazon. Identifica de forma inequívoca un recurso de AWS.
- Clave de contenido: clave criptográfica que se utiliza para cifrar parte del contenido.
- Proveedor de contenido: un publicador que proporciona los derechos y las reglas para la distribución de contenido multimedia protegido. El proveedor de contenido también puede

proporcionar el contenido multimedia de origen (formato intermedio, para la transcodificación), identificadores de activos, identificadores clave (KIDs), valores clave, instrucciones de codificación y metadatos de descripción del contenido.

- DRM: administración de derechos digitales. Se utiliza para proteger el contenido digital protegido por derechos de autor frente a accesos sin autorización.
- Plataforma DRM: un sistema que proporciona compatibilidad y funcionalidad de DRM a los usuarios y encriptadores, además de proporcionar claves de DRM y licencias para el cifrado y descifrado de contenido.
- Proveedor de DRM: consulte la plataforma DRM.
- Sistema DRM: estándar para las implementaciones de DRM. Los sistemas DRM más comunes incluyen Apple FairPlay, Google Widevine y Microsoft. PlayReady Los proveedores de contenido utilizan los sistemas DRM para proteger el contenido digital para su entrega a los usuarios y para el acceso por parte de ellos. Para obtener una lista de los sistemas DRM registrados en DASH-IF, consulte Sistema DASH-IF. IDs La especificación DASH-IF CPIX utiliza el término "sistema DRM" tal como se lo define aquí y, en algunos casos, utiliza "sistema DRM" para referirse a lo que esta especificación denomina plataforma DRM.
- Solución DRM: consulte la plataforma DRM.
- Tecnología DRM: consulte el sistema DRM.
- Encriptador: un componente de procesamiento multimedia que cifra el contenido multimedia con claves obtenidas del proveedor de claves. Por lo general, los encriptadores también añaden a los medios la señalización de cifrado DRM y los metadatos. Los encriptadores suelen ser codificadores, empaquetadores y transcodificadores.
- Proveedor de claves: el componente de una plataforma DRM que expone una API de REST de SPEKE para gestionar las solicitudes de claves. El proveedor de claves podría ser el propio servidor de claves o podría ser otro componente de la plataforma.
- Servidor de claves: el componente de una plataforma DRM que mantiene las claves para el cifrado y descifrado del contenido.
- Operador: una persona encargada de operar todo el sistema, incluidos el encriptador y el proveedor de claves.
- Reproductor: un reproductor multimedia que funciona en nombre de un usuario. Obtiene la información de distintas fuentes, incluidos los archivos de manifiesto multimedia, los archivos multimedia y las licencias DRM. Solicita licencias de la plataforma DRM en nombre de los usuarios.

Incorporación de clientes a SPEKE

Proteja su contenido de usos no autorizados al combinar un proveedor de claves de sistema de gestión de derechos digitales (DRM) de Secure Packager and Encoder Key Exchange (SPEKE) con su encriptador y con sus reproductores multimedia. (SPEKE) define el estándar para la comunicación entre los encriptadores y los empaquetadores de contenido multimedia y proveedores de claves de gestión de derechos digitales (DRM). Para acceder, elija un proveedor de claves de plataforma DRM y configure la comunicación entre el proveedor de claves y sus encriptadores y reproductores.

Temas

Comience con un proveedor de plataformas DRM

Los siguientes socios de Amazon proporcionan implementaciones de plataforma DRM de terceros para SPEKE. Para obtener más información sobre las ofertas y la información de contacto, siga los enlaces a las páginas de la Red de socios de Amazon. Los socios sin enlace no disponen actualmente de una página en la Red de socios de Amazon, pero puede contactarlos de forma directa. Los socios pueden ayudarlo a prepararse para utilizar sus plataformas.

Proveedor de plataformas DRM	Soporte SPEKE v1	Soporte SPEKE v2
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
DOVERUNNER	√	√

Proveedor de plataformas DRM	Soporte SPEKE v1	Soporte SPEKE v2
Insys Cloud DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√
JW Player	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

Soporte de SPEKE en los servicios y productos de AWS

En esta sección se muestra el soporte SPEKE proporcionado por los servicios multimedia de AWS que se ejecutan en la Nube de AWS y por los productos multimedia en las instalaciones de AWS. Estos servicios y productos son los encriptadores dentro de la arquitectura de cifrado de contenido SPEKE. Asegúrese de que el protocolo de streaming y el sistema DRM que quiere utilizar estén disponibles para su servicio o producto.

Servicio o producto de AWS	Soporte SPEKE v1	Soporte SPEKE v2	Tecnologías DRM compatibles
AWS Elemental MediaConvert : servicio que se	√	√	Documentación

Servicio o producto de AWS	Soporte SPEKE v1	Soporte SPEKE v2	Tecnologías DRM compatibles
ejecuta en la nube de AWS			
AWS Elemental MediaPackage : servicio que se ejecuta en la nube de AWS	√	√	Documentación
AWS Elemental Live: producto local	√		Documentación: MPEG-DASH / HLS
AWS Elemental Server: producto local	√		Documentación

Soporte de SPEKE en los servicios y productos de los socios de AWS

En esta sección se muestra el soporte SPEKE proporcionado por los servicios y productos de los socios de AWS que se ejecutan en la nube de AWS. Estos servicios y productos son los encriptadores dentro de la arquitectura de cifrado de contenido SPEKE. Asegúrese de que el protocolo de streaming y el sistema DRM que quiere utilizar estén disponibles para su servicio o producto.

Servicio o producto de AWS	Soporte SPEKE v1	Soporte SPEKE v2	Tecnologías DRM compatibles
Codificación de vídeo en directo con Bitmovin	√		Documentación
Codificación de vídeo bajo demanda (VOD) con Bitmovin	√		Documentación

Especificación de la API de SPEKE

Esta es la especificación de la API de REST para Secure Packager and Encoder Key Exchange (SPEKE). Utilice esta especificación para ofrecer protección de derechos de autor DRM a los clientes que utilicen el cifrado.

En un flujo de trabajo de streaming de vídeo, el motor de cifrado se comunica con el proveedor de claves de la plataforma DRM para solicitar claves de contenido. Estas claves son sumamente confidenciales, por lo que es fundamental que el proveedor de claves y el motor de cifrado establezcan un canal de comunicación de confianza que sea altamente seguro. También puede cifrar las claves de contenido del documento para obtener un end-to-end cifrado más seguro.

Esta especificación persigue los siguientes objetivos:

- Definir una interfaz sencilla, de confianza y con un alto nivel de seguridad que los proveedores y clientes de DRM puedan utilizar para integrarla con los encriptadores cuando sea necesario cifrar el contenido.
- Abarcar flujos de trabajo de VOD y en directo e incluir las condiciones de error y los mecanismos de autenticación necesarios para establecer una comunicación sólida y altamente segura entre los encriptadores y los puntos de enlace del proveedor de claves de DRM.
- Incluye soporte para los empaques HLS, MSS y DASH y sus sistemas DRM habituales: FairPlay, PlayReady y WideVine/CENC.
- Conseguir que la especificación sea sencilla y pueda ampliarse para admitir futuros sistemas DRM.
- Utilizar una API de REST sencilla.

> **Note**
>
>

SEAN CONTRACTUALES EXTRACONTRACTUALES O DE OTRA ÍNDOLE, DERIVADOS DEL MATERIAL O RELACIONADOS CON ÉL, CON SU UTILIZACIÓN O CON OTROS USOS DE ESTE.

Temas

Se requiere autenticación para SPEKE

SPEKE requiere autenticación para los productos en las instalaciones y para los servicios y características que se ejecutan en la nube de AWS.

Temas

Autenticación para implementaciones en la nube de AWS

SPEKE requiere la autenticación de AWS a través de roles de IAM cuando se utiliza un encriptador. Los roles de IAM los crea el proveedor de DRM o el operador que es propietario del punto de enlace de DRM de una cuenta de AWS. A cada rol se le asigna un nombre de recurso de Amazon (ARN). Este ARN lo proporciona el operador del servicio de AWS Elemental en la consola del servicio al solicitar el cifrado. Es necesario configurar los permisos de la política del rol para permitir el acceso a la API del proveedor de claves, pero no a ningún otro recurso de AWS. Cuando el encriptador se contacta con el proveedor de claves de DRM, utiliza el ARN del rol para adoptar el rol del titular de la cuenta del proveedor de claves, que devuelve credenciales temporales para el encriptador que se van a utilizar a fin de obtener acceso al proveedor de claves.

Una de las implementaciones más habituales tiene como objetivo que el operador o el proveedor de la plataforma DRM utilicen Amazon API Gateway delante del proveedor de claves y, a continuación, habiliten la autorización de AWS Identity and Access Management (AWS IAM) en el recurso de

API Gateway. Puede utilizar la siguiente definición de política de ejemplo y asociarla al nuevo rol para conceder permisos a los recursos adecuados. En este caso, los permisos son para todos los recursos de API Gateway.

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

Por último, el rol necesita que se incluya una relación de confianza, por lo que es necesario que el operador pueda seleccionar el servicio.

En el ejemplo siguiente, se muestra el ARN de un rol que se ha creado para obtener acceso al proveedor de claves de DRM:

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

Para obtener más información sobre la creación de un rol, consulte AWS AssumeRole. Para obtener más información acerca de la firma de solicitudes, consulte AWS Sigv4.

Autenticación de productos en las instalaciones

En el caso de los productos en las instalaciones, le recomendamos que utilice SSL/TLS y la autenticación de resumen para obtener la mejor seguridad, pero como mínimo debe utilizar la autenticación básica a través de HTTPS.

Los dos tipos de autenticación utilizan el encabezado `Authorization` en la solicitud HTTP:

- Resumen de autenticación: el encabezado de autorización consta del identificador `Digest` seguido de una serie de valores que autentican la solicitud. Concretamente, el valor de respuesta se genera mediante una serie de funciones de MD5 hash que incluyen una función única, la cual

one-time-use no proviene del servidor, y que se utiliza para garantizar que la contraseña circule de forma segura.

- Autenticación básica: el encabezado de autorización consta del identificador `Basic` seguido de una cadena codificada en base-64 que representa el nombre de usuario y la contraseña, separados por dos puntos.

Para obtener más información acerca de la autenticación básica e implícita, incluida información detallada sobre el encabezado, consulte la especificación del Grupo de trabajo de ingeniería de Internet (IETF) RFC 2617 - HTTP Autenticación: autenticación de acceso básica y recopilada.

SPEKE API v1

Esta es la API REST para Secure Packager and Encoder Key Exchange (SPEKE) v1. Utilice esta especificación para ofrecer protección de derechos de autor DRM a los clientes que utilicen el cifrado. Para que sea compatible con SPEKE, su proveedor de claves DRM debe exponer la API de REST que se describe en esta especificación. El encriptador realiza llamadas a API al proveedor de claves.

> **Note**
>
> Los ejemplos de código de esta especificación se proporcionan únicamente con fines ilustrativos. Los ejemplos no pueden ejecutarse porque no conforman una implementación de SPEKE completa.

SPEKE utiliza la definición de estructura de datos del DASH Industry Forum Content Protection Information Exchange Forum (DASH-IF-CPIX) para el intercambio de claves, con algunas restricciones. DASH-IF-CPIXdefine un esquema para proporcionar un intercambio extensible y multiDRM desde la plataforma DRM hasta el cifrador. Esto permite cifrar el contenido en todos los formatos de empaquetado con velocidades de bits adaptativas en el momento en que se comprime y empaqueta el contenido. Los formatos de empaquetamiento con velocidades de bits adaptativas son HLS, DASH y MSS.

Para obtener información detallada sobre el formato de intercambio, consulte la especificación CPIX del DASH Industry Forum en https://dashif. org/docs/DASH-IF-CPIX-v2-0.pdf.

Temas

SPEKE API v1: personalizaciones y restricciones a la especificación de DASH-IF

La especificación CPIX de DASH-IF, https://dashif. org/docs/DASH-IF-CPIX-v2-0.pdf admite varios casos de uso y topologías. La especificación de API de SPEKE se ajusta a la especificación CPIX con las siguientes personalizaciones y restricciones:

- SPEKE sigue el flujo de trabajo Encriptador-Consumidor.
- En las claves de contenido cifradas, SPEKE aplica las siguientes restricciones:
  - SPEKE no admite la verificación de firma digital (XMLDSIG) para cargas de solicitud o respuesta.
  - SPEKE requiere 2048 certificados basados en RSA.
- En los flujos de trabajo de rotación de claves, SPEKE requiere el filtro `ContentKeyUsageRule`, `KeyPeriodFilter`. SPEKE omite todos los demás ajustes `ContentKeyUsageRule`.
- SPEKE omite la funcionalidad `UpdateHistoryItemList`. Si la lista está presente en la respuesta, SPEKE la omite.
- SPEKE admite la rotación de claves. SPEKE utiliza únicamente el `ContentKeyPeriod@index para realizar un seguimiento del período clave.
- Para admitir MSS PlayReady, SPEKE usa un parámetro personalizado debajo de la `DRMSystem` etiqueta,. `SPEKE:ProtectionHeader`
- En el empaquetado HLS, si `URIExtXKey` está presente en la respuesta, debe contener todos los datos que se van a agregar en el parámetro de la etiqueta `EXT-X-KEY` del URI como una lista de reproducción de HLS, sin ningún otro requisito de señalización.

- En la lista de reproducción de HLS, en la etiqueta `DRMSystem`, SPEKE proporciona los parámetros personalizados opcionales `speke:KeyFormat` y `speke:KeyFormatVersions` para los valores de los parámetros `KEYFORMAT` y `KEYFORMATVERSIONS` de la etiqueta `EXT-X-KEY`.

  El vector de inicialización (IV) de HLS siempre sigue el número de segmentos a menos que el operador lo especifique de forma explícita.
- Al solicitar claves, el encriptador puede utilizar el atributo `@explicitIV` opcional en el elemento `ContentKey`. El proveedor de claves puede responder con un IV mediante `@explicitIV`, aunque el atributo no esté incluido en la solicitud.
- El encriptador crea el identificador de la clave (`KID`), que es el mismo para cualquier ID de contenido y periodo de clave especificados. El proveedor de claves incluye el `KID` en la respuesta al documento de solicitud.
- El proveedor de claves podría incluir un valor para el encabezado de respuesta de `Speke-User-Agent` a fin de que se identifique con fines de depuración.
- Actualmente, SPEKE no admite varios seguimientos o claves por contenido.

  El encriptador compatible con SPEKE actúa como cliente y envía operaciones `POST` al punto de conexión del proveedor de claves. El encriptador podría enviar una solicitud `heartbeat` periódica para asegurarse de que la conexión entre el encriptador y el punto de conexión del proveedor de claves está en buen estado.

SPEKE API v1: componentes de carga estándar

En cualquier solicitud de SPEKE, el encriptador puede solicitar respuestas de uno o varios sistemas DRM. El encriptador especifica los sistemas DRM en `<cpix:DRMSystemList>` de la carga de la solicitud. Cada especificación del sistema incluye la clave e indica el tipo de respuesta que se va a devolver.

En el siguiente ejemplo, se muestra una lista de sistemas DRM con una única especificación:

```
<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>
```

En la siguiente tabla, se muestran los componentes principales de cada `<cpix:DRMSystem>`.

Identificador	Descripción
`systemId` o `schemeId`	Identificador único del tipo de sistema DRM, tal como se registró con la organización de DASH IF. Para ver una lista, consulte Sistema DASH-IF. IDs
`kid`	ID de la clave. Esta no es la clave real, sino un identificador que apunta a la clave de una tabla hash.
`<cpix:UriExtXKey>`	Solicita una clave estándar no cifrada. El tipo de respuesta de clave debe ser esta o la respuesta `PSSH`.
`<cpix:PSSH>`	Solicita un encabezado específico del sistema de protección (PSSH). Este tipo de encabezado contiene una referencia al `kid`, `systemID`, así como datos personalizados sobre el proveedor de DRM, como parte de Common Encryption (CENC). El tipo de respuesta de clave debe ser esta o la respuesta `UriExtXKey` .

_Ejemplo de solicitudes de clave estándar y PSSH _

En el siguiente ejemplo se muestra parte de una solicitud de ejemplo procedente del encriptador y dirigida al proveedor de claves de DRM, con los componentes principales resaltados. La primera solicitud es para a una clave estándar, mientras que la segunda es para una respuesta PSSH:

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

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

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

_Ejemplo de respuestas de una clave estándar y PSSH _

En el ejemplo siguiente se muestra la respuesta correspondiente del proveedor de claves de DRM al encriptador:

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

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

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

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

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

SPEKE API v1: ejemplos de llamadas al método de flujo de trabajo en directo

Ejemplo de la sintaxis de la solicitud

La siguiente URL es un ejemplo y no indica un formato fijo:

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

Cuerpo de la solicitud

Un elemento CPIX.

Encabezados de la solicitud

Nombre	Tipo	Se ejecuta	Descripción
`AWS Authorization`	Cadena	1..1	Consulte AWS Sigv4
`X-Amz-Security-Token`	Cadena	1..1	Consulte AWS Sigv4
`X-Amz-Date`	Cadena	1..1	Consulte AWS Sigv4
`Content-Type`	Cadena	1..1	application/xml

Encabezados de la respuesta

Nombre	Tipo	Se ejecuta	Descripción
`Speke-User-Agent`	Cadena	1..1	Cadena que identifica al proveedor de claves
`Content-Type`	Cadena	1..1	application/xml

Respuesta a la solicitud

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	Respuesta de la carga de DASH-CPIX
`4XX (Client error)`	Mensaje de error del cliente	1..1	Descripción del error del cliente
`5XX (Server error)`	Mensaje de error del servidor	1..1	Descripción del error del servidor

> **Note**
>
> Los ejemplos que aparecen en esta sección no incluyen el cifrado de las claves de contenido. Para obtener información acerca de cómo agregar el cifrado de claves de contenido, consulte Cifrado de claves de contenido.

Carga de solicitud de ejemplo en directo con claves sin cifrar

En el siguiente ejemplo se muestra una carga típica de solicitud en directo desde el encriptador al proveedor de claves DRM:

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

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

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

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

Carga de respuesta de ejemplo en directo con claves sin cifrar

En el siguiente ejemplo se muestra una carga normal de una respuesta del proveedor de claves de DRM:

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

 <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIExtXKey>
```

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

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

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

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

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

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

 <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4IhflQAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAcA
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
```

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

SPEKE API v1: ejemplos de llamadas de método de flujo de trabajo VOD

Ejemplo de la sintaxis de la solicitud

La siguiente URL es un ejemplo y no indica un formato fijo.

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

Cuerpo de la solicitud

Un elemento CPIX.

Encabezados de la respuesta

Nombre	Tipo	Se ejecuta	Descripción
`Speke-User-Agent`	Cadena	1..1	Cadena que identifica al proveedor de claves
`Content-Type`	Cadena	1..1	application/xml

Respuesta a la solicitud

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	Respuesta de la carga de DASH-CPIX
`4XX (Client error)`	Mensaje de error del cliente	1..1	Descripción del error del cliente

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`5XX (Server error)`	Mensaje de error del servidor	1..1	Descripción del error del servidor

> **Note**
>
> Los ejemplos que aparecen en esta sección no incluyen el cifrado de las claves de contenido. Para obtener información acerca de cómo agregar el cifrado de claves de contenido, consulte Cifrado de claves de contenido.

Carga de solicitud de ejemplo de VOD con claves sin cifrar

En el siguiente ejemplo se muestra una carga de solicitud VOD básica del encriptador al proveedor de claves 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>
```

Carga de respuesta de ejemplo de VOD con claves sin cifrar

En el ejemplo siguiente se muestra una carga de respuesta de VOD básica procedente del proveedor de claves de DRM:

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

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

```
  </cpix:DRMSystem>

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

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

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

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

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

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

SPEKE API v1: cifrado de claves de contenido

Si lo desea, puede añadir el cifrado de claves de contenido en la implementación de SPEKE. El cifrado de claves de contenido garantiza una end-to-end protección total al cifrar las claves de

contenido para el tránsito, además de cifrar el contenido en sí. Si no implementa esta funcionalidad para su proveedor de claves, debe utilizar el cifrado de capa de transporte junto con un sólido mecanismo de autenticación para garantizar la seguridad.

Para utilizar el cifrado de claves de contenido para los cifradores que se ejecutan en la nube de AWS, los clientes importan los certificados al AWS Certificate Manager y, a continuación, utilizan el certificado resultante ARNs para sus actividades de cifrado. El cifrador utiliza el certificado ARNs y el servicio ACM para proporcionar claves de contenido cifrado al proveedor de claves DRM.

Restricciones

SPEKE admite el cifrado de claves de contenido tal y como se establece en la especificación DASH-IF CPIX con las siguientes restricciones:

- SPEKE no admite la verificación de firma digital (XMLDSIG) para cargas de solicitud o respuesta.
- SPEKE requiere 2048 certificados basados en RSA.

Estas restricciones también se enumeran en Personalizaciones y restricciones a la especificación DASH-IF.

Implementación del cifrado de claves de contenido

Para proporcionar el cifrado de claves de contenido, haga lo siguiente en las implementaciones del proveedor de claves de DRM:

- Administre el elemento `<cpix:DeliveryDataList>` en las cargas de las solicitudes y las respuestas.
- Proporcione valores cifrados en el elemento `<cpix:ContentKeyList>` de las cargas de respuesta.

Para obtener más información sobre estos elementos, consulte la especificación DASH-IF CPIX 2.0.

Ejemplo del elemento `<cpix:DeliveryDataList>` de cifrado de claves de contenido en la carga de una solicitud

En el siguiente ejemplo se resalta el elemento `<cpix:DeliveryDataList>` en negrita:

```
<?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>
```

Ejemplo del elemento `<cpix:DeliveryDataList>` de cifrado de claves de contenido en la carga de una respuesta

En el siguiente ejemplo se resalta el elemento `<cpix:DeliveryDataList>` en negrita:

```
<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>
```

Ejemplo del elemento `<cpix:ContentKeyList>` de cifrado de claves de contenido en la carga de una respuesta

En el ejemplo siguiente se muestra la gestión de las claves de contenido cifradas en el elemento `<cpix:ContentKeyList>` de la carga de respuesta. Aquí se utiliza el 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>
```

En comparación, el siguiente ejemplo muestra una carga de respuesta similar con la clave de contenido entregada sin cifrar, como una clave sin cifrar. Aquí se utiliza el elemento `<pskc:PlainValue>`:

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

API SPEKE v1: latido

Ejemplo de la sintaxis de la solicitud

La siguiente URL es un ejemplo y no indica un formato fijo:

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

Respuesta a la solicitud

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	statusMessage	1..1	Mensaje que describe el estado.

API SPEKE v1: anulación del identificador clave

El encriptador crea un nuevo identificador de clave (KID) cada vez que se modifican las claves. A continuación, pasa el KID al servidor de claves de DRM en las solicitudes. Casi siempre, el servidor de claves responde utilizando el mismo KID, aunque puede proporcionar un valor de KID diferente en la respuesta.

A continuación, se muestra un ejemplo de una solicitud con el 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 siguiente respuesta invalida el KID por `22222222-2222-2222-2222-222222222222`:

```
    <cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
     <cpix:ContentKeyList>
```

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

SPEKE API v2

Esta es la API REST para Secure Packager and Encoder Key Exchange (SPEKE) v2. Utilice esta especificación para ofrecer protección de derechos de autor DRM a los clientes que utilicen el cifrado. Para que sea compatible con SPEKE, su proveedor de claves DRM debe exponer la API de REST que se describe en esta especificación. El encriptador realiza llamadas a API al proveedor de claves.

> **Note**
>
> Los ejemplos de código de esta especificación se proporcionan únicamente con fines ilustrativos. Los ejemplos no pueden ejecutarse porque no conforman una implementación de SPEKE completa.

SPEKE utiliza la definición de estructura de datos del DASH Industry Forum Content Protection Information Exchange Forum (DASH-IF-CPIX) para el intercambio de claves, con algunas restricciones. DASH-IF-CPIXdefine un esquema para proporcionar un intercambio extensible y multiDRM desde la plataforma DRM hasta el cifrador. Esto permite cifrar el contenido en todos los formatos de empaquetado con velocidades de bits adaptativas en el momento en que se comprime y empaqueta el contenido. Los formatos de empaquetamiento con velocidades de bits adaptativas son HLS, DASH y MSS.

A partir de su versión 2.0, SPEKE se alinea con una versión específica del CPIX:

Por el lado de SPEKE, esto se aplica mediante el uso del encabezado HTTP `X-Speke-Version` y, por el lado del CPIX, mediante el uso del atributo `CPIX@version`. La ausencia de estos elementos en las solicitudes es algo habitual en los flujos de trabajo heredados de SPEKE v1. En los flujos de trabajo de SPEKE v2, se espera que el proveedor de claves procese los documentos CPIX solo si admite ambos parámetros de la versión.

Para obtener información detallada acerca del formato de intercambio, consulte la especificación CPIX 2.3 DASH Industry Forum.

En general, SPEKE v2.0 presenta las siguientes evoluciones en comparación con SPEKE v1.0:

- Todas las etiquetas del espacio de nombres XML de SPEKE están obsoletas en favor de etiquetas equivalentes en el espacio de nombres XML de CPIX
- `SPEKE:ProtectionHeader` está obsoleta y se sustituye con `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`, `SPEKE:KeyFormat` y `SPEKE:KeyFormatVersions` están obsoletas y se sustituyen con `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id` se sustituye con `CPIX@contentId`
- Nuevos atributos CPIX obligatorios: `CPIX@version`, `ContentKey@commonEncryptionScheme`
- Nuevo elemento CPIX opcional: `DRMSystem.ContentProtectionData`
- Soporte para múltiples claves de contenido

- Mecanismo de control de versiones cruzado entre SPEKE y CPIX
- Evolución de los encabezados HTTP: nuevo encabezado `X-Speke-Version`, encabezado `Speke-User-Agent` renombrado como `X-Speke-User-Agent`
- Latido de la API obsoleto

Como la especificación SPEKE v1.0 permanece inalterada, no es necesario cambiar las implementaciones existentes para que sigan siendo compatibles con los flujos de trabajo de SPEKE v1.0.

Temas

SPEKE API v2: personalizaciones y restricciones a la especificación de DASH-IF

La especificación CPIX 2.3 DASH Industry Forum admite una serie de casos de uso y topologías. La especificación SPEKE API v2.0 define tanto un perfil CPIX como una API para CPIX. Para alcanzar estos dos objetivos, se ajusta a la especificación CPIX con las siguientes personalizaciones y restricciones:

Perfil CPIX

- SPEKE sigue el flujo de trabajo Encriptador-Consumidor.
- En las claves de contenido cifradas, SPEKE aplica las siguientes restricciones:
  - SPEKE no admite la verificación de firma digital (XMLDSIG) para cargas de solicitud o respuesta.
  - SPEKE requiere 2048 certificados basados en RSA.
- SPEKE aprovecha solo un subconjunto de funcionalidades del CPIX:

  - SPEKE omite la funcionalidad `UpdateHistoryItemList`. Si la lista está presente en la respuesta, SPEKE la omite.
  - SPEKE omite la funcionalidad de las claves raíz/hoja. Si el atributo `ContentKey@dependsOnKey` está presente en la respuesta, SPEKE la omite.
  - SPEKE omite el elemento `BitrateFilter` y el atributo `VideoFilter@wcg`. Si estos elementos o atributos están presentes en la carga del CPIX, SPEKE los omite.
- En los documentos del CPIX intercambiados con SPEKE v2, solo se pueden utilizar los elementos o atributos a los que se hace referencia como “compatibles” en la página de componentes de carga estándar o en la página del contrato de cifrado.
- Cuando el encriptador los incluya en una solicitud de CPIX, todos los elementos y atributos deberán incluir un valor válido en la respuesta del CPIX del proveedor de claves. De lo contrario, el encriptador se detendrá y generará un error.
- SPEKE admite la rotación de claves con elementos `KeyPeriodFilter`. SPEKE utiliza únicamente el `ContentKeyPeriod@index` para realizar un seguimiento del período clave.
- Para la señalización HLS, se deben utilizar varios elementos `DRMSystem.HLSSignalingData`: uno con el valor de atributo `DRMSystem.HLSSignalingData@playlist` de “multimedia” y otro con un valor de atributo `DRMSystem.HLSSignalingData@playlist` de “maestro”.
- Al solicitar claves, el encriptador puede utilizar el atributo `@explicitIV` opcional en el elemento `ContentKey`. El proveedor de claves puede responder con un IV mediante `@explicitIV`, aunque el atributo no esté incluido en la solicitud.
- El encriptador crea el identificador de la clave (`KID`), que es el mismo para cualquier ID de contenido y periodo de clave especificados. El proveedor de claves incluye el `KID` en la respuesta al documento de solicitud.
- El encriptador incluirá un valor para el atributo `CPIX@contentId`. Al recibir un valor vacío para este atributo, el proveedor de claves devolverá un error con la descripción “Missing CPIX@contentId” (Falta CPIX@contentId). El proveedor de claves no puede anular un valor `CPIX@contentId`.

  El proveedor de claves ignorará el valor `CPIX@id` si no es nulo.
- El encriptador incluirá un valor para el atributo `CPIX@version`. Al recibir un valor vacío para este atributo, el proveedor de claves devolverá un error con la descripción “Missing CPIX@version” (Falta CPIX@version). Al recibir una solicitud con una versión no compatible, la descripción del error devuelta por el proveedor de claves será “Unsupported CPIX@version” (CPIX@version no compatible).

El proveedor de claves no puede anular un valor `CPIX@version`.

- El encriptador incluirá un valor para el atributo `ContentKey@commonEncryptionScheme` de cada clave solicitada. Al recibir un valor vacío para este atributo, el proveedor de claves devolverá un error con la descripción « ContentKeyFalta @ para KID». commonEncryptionScheme `id`

  Un documento CPIX único no puede mezclar varios valores para distintos atributos `ContentKey@commonEncryptionScheme`. Al recibir dicha combinación, el proveedor de claves devolverá un error con la descripción «Combinación ContentKey @ commonEncryptionScheme no conforme».

  No todos los valores `ContentKey@commonEncryptionScheme` son compatibles con todas las tecnologías DRM. Al recibir una combinación de este tipo, el proveedor de claves devolverá un error con la descripción «ContentKey@ commonEncryptionScheme no compatible con DRMSystem `id`».

  El proveedor de claves no puede anular un valor `ContentKey@commonEncryptionScheme`.
- Al recibir valores diferentes para elemento <pssh> innerXML `DRMSystem@PSSH` y `DRMSystem.ContentProtectionData` en el cuerpo de la respuesta del CPIX, el encriptador se detendrá y generará un error.

API para CPIX

- El proveedor de claves debe incluir un valor para el encabezado de respuesta HTTP `X-Speke-User-Agent`.
- Un encriptador compatible con SPEKE actúa como cliente y envía operaciones de POST al punto de conexión del proveedor de claves.
- El cifrador incluirá un valor para el encabezado de la solicitud `X-Speke-Version` HTTP, y la versión SPEKE utilizada en la solicitud se formulará como. MajorVersion MinorVersion, como «2.0» para SPEKE v2.0. Si el proveedor de claves no admite la versión SPEKE utilizada por el encriptador para la solicitud actual, devolverá un error con la descripción “Unsupported SPEKE version” (versión no compatible con SPEKE) y en la medida de lo posible no procesará el documento CPIX.

  El proveedor de claves no puede modificar el valor del encabezado `X-Speke-Version` definido por el encriptador en respuesta a la solicitud.

- Al recibir errores en el cuerpo de la respuesta, el encriptador emitirá un error y no volverá a intentar la solicitud con un control de versión SPEKE v1.0.

  Si el proveedor de claves no arroja error, pero no devuelve un documento CPIX que incluya la información obligatoria, el encriptador debería detenerse y generar un error.

La siguiente tabla resume los mensajes estándar que debe devolver el proveedor de claves en el cuerpo del mensaje. En caso de error, el código de respuesta HTTP debe ser 4XX o 5XX, nunca 200. El código de error 422 se puede utilizar para todos los errores relacionados con SPEKE/CPIX.

Caso de error	Mensaje de error
CPIX @contentId no está definido	Falta CPIX @contentId
CPIX @version no está definido	Falta CPIX @version
No se admite CPIX @version	CPIX@version no es compatible
ContentKey@ no commonEncryptionScheme está definido	Falta ContentKey @ commonEncryptionScheme para KID `id` (donde `id` es igual al valor ContentKey @kid)
Se utilizan varios commonEncryptionScheme valores ContentKey @ en un único documento CPIX	Combinación @ no compatible ContentKey commonEncryptionScheme
ContentKey@ no commonEncryptionScheme es compatible con la tecnología DRM	ContentKey@ commonEncryptionScheme no es compatible con DRMSystem `id` (donde `id` es igual al valor DRMSystem @systemId)
X-Speke-Version el valor del encabezado no es una versión de SPEKE compatible	La versión de SPEKE no es compatible
El contrato de cifrado es incorrecto	Contrato de cifrado con formato incorrecto
El contrato de cifrado contradice las restricciones de los niveles de seguridad del DRM	No se admite el contrato de cifrado CPIX solicitado

Caso de error	Mensaje de error
El contrato de cifrado no incluye ningún elemento VideoFilter o elemento AudioFilter	Falta el contrato de cifrado CPIX

SPEKE API v2: componentes de carga estándar

A través de una única solicitud SPEKE, el encriptador puede solicitar múltiples claves de contenido, junto con la señalización manifiesta necesaria para varios formatos de empaquetado, de acuerdo con el contrato de cifrado definido para un contenido determinado.

Para cubrir todos estos aspectos, un documento CPIX estándar se compone de tres secciones de lista obligatorias, además de una sección de lista opcional para la rotación de claves de contenido en directo.

<cpix:CPIX><cpix: ContentKeyList > sección y elemento de nivel superior

Se trata de una sección obligatoria, relevante tanto para la transmisión en directo como para la de vídeo bajo demanda, en la que se definen las diferentes claves de contenido que debe utilizar el encriptador. El elemento `<cpix:ContentKeyList>` puede contener uno o varios elementos secundarios `<cpix:ContentKey>`, cada uno de los cuales describe una clave de contenido distinta.

Según la especificación CPIX, los posibles valores del atributo `ContentKey@commonEncryptionScheme` se definen en la especificación sobre el cifrado común en los archivos con formato de archivo multimedia de base ISO (ISO/IEC 23001-7:2016):

- 'cenc': cifrado de muestra completa y submuestra NAL de vídeo en modo AES-CTR
- 'cbc1': cifrado de muestra completa y submuestra NAL de vídeo en modo AES-CBC
- 'cens': cifrado de patrón NAL de vídeo parcial en modo AES-CTR
- 'cbcs': cifrado de patrón NAL de vídeo parcial en modo AES-CBC

El siguiente ejemplo muestra un documento CPIX con una única clave de contenido no cifrada:

```
<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>
```

De forma predeterminada, las claves de contenido no están cifradas, como en el siguiente ejemplo. Sin embargo, el cifrador puede solicitar el cifrado de las claves de contenido mediante la inclusión del elemento<cpix : >. DeliveryDataList Consulte la sección de cifrado de claves de contenido para obtener más información.

Elemento compatible con SPEKE	Atributos obligatorios	Atributos opcionales	Elementos secundarios obligatorios	Elementos secundarios opcionales
<cpix:CPIX>	ID de contenido , versión, xmlns:cpix, xmlns:pskc	nombre, xmlns:enc	uno <cpix: ContentKeyList >, uno<cpix : List>, uno <cpix : >DRMSyste mContentK eyUsageRuleList	uno <cpix: DeliveryDataList ContentKe yPeriodList >, uno <cpix : >
<cpixCont entKeyList: >	-	id	al menos un <cpix : >ContentKey	-
<cpix : >ContentKey	niño, Data commonEnc ryptionScheme	id, algoritmo, ExpliciTiv	un <pskc:Sec ret>	-
<pskc:Secret>	PlainValue o bien Encrypted Value	Valor MAC	-	<enc: Encryptio nMethod >, <enc : >CipherData

<cpix: sección List> DRMSystem

Esta es una sección obligatoria, relevante tanto para la transmisión en vivo como para la transmisión bajo demanda, que define los diferentes sistemas DRM que deben aprovecharse junto con las claves de contenido.

El siguiente ejemplo muestra una lista de sistemas DRM con una única especificación de sistema DRM: PlayReady

```
<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>
```

Para obtener una lista completa de los sistemas DRMIDs, consulte la sección de protección de contenido del repositorio de identificadores DASH-IF.

Elemento compatible con SPEKE	Atributos obligatorios	Atributos opcionales	Elementos secundarios obligatorios	Elementos secundarios opcionales
<cpix : List>DRMSystem	-	id	al menos un <cpix : >DRMSystem	-
<cpix : >DRMSystem	kid, SystemID	id, nombre, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHeaderData, dos elementos de

Elemento compatible con SPEKE	Atributos obligatorios	Atributos opcionales	Elementos secundarios obligatorios	Elementos secundarios opcionales
				<cpix: HLSSignaling Data> con un valor de atributo de lista de reproducción diferente

`DRMSystem@PSSH` es obligatorio si la encapsulación ISO-BMFF se aplica a los segmentos multimedia. El encriptador aprovecha el `DRMSystem.ContentProtectionData` elemento innerXML `<pssh>` solo con fines de señalización de manifiestos.

Si `DRMSystem@PSSH` está presente y `DRMSystem.ContentProtectionData` contiene un elemento `<pssh>` innerXML, ambos valores deberán ser idénticos.

Si la señalización `DRMSystem` se va a incluir en los manifiestos HLS, se deben incluir tanto los elementos `<cpix:HLSSignalingData playlist="media">` como los `<cpix:HLSSignalingData playlist="master">` en la solicitud y la respuesta del CPIX.

sección <cpix : >ContentKeyPeriodList

Esta es una sección opcional, relevante solo para la transmisión en vivo, que define los períodos criptográficos que se aplican al contenido.

El elemento `<cpix:ContentKeyPeriodList>` puede contener uno o varios elementos secundarios `<cpix:ContentKeyPeriod>`, cada uno de los cuales describe un periodo de cifrado distinto en la cronología en directo. UUIDs Usarlo como parte del valor del atributo id es un enfoque que se utiliza habitualmente.

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

Elemento compatible con SPEKE	Atributos obligatorios	Atributos opcionales	Elementos secundarios obligatorios	Elementos secundarios opcionales
<cpix : >ContentKeyPeriodList	-	id	al menos un <cpix : >ContentKeyPeriod	-
<cpix : >ContentKeyPeriod	id, índice	-	-	-

Si se utilizan períodos de cifrado, las claves de cifrado también deben adjuntarse a uno de los períodos cifrados del documento CPIX, como se muestra en la siguiente sección.

sección <cpix : >ContentKeyUsageRuleList

Se trata de una sección obligatoria, relevante tanto para el streaming en directo como para el de vídeo bajo demanda, en la que se define cómo las diferentes claves de contenido protegerán las pistas incluidas en el streamset y en todos los períodos cifrados.

El elemento <cpix: ContentKeyUsageRuleList > puede contener uno o varios elementos secundarios de <cpix: ContentKeyUsageRule >, y cada uno de ellos describe las pistas a las que el cifrador aplica una clave de contenido determinada, posiblemente durante un período de cifrado específico. Es necesario que haya al menos un elemento <cpix: AudioFilter > o un <cpix : >en un elemento <cpix: VideoFilter >. ContentKeyUsageRule

El siguiente ejemplo muestra una lista sencilla con una sola regla que aplica una única clave de contenido a todas las pistas de audio y vídeo durante un periodo de cifrado específico.

```
<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 compatible con SPEKE	Atributos obligatorios	Atributos opcionales	Elementos secundarios obligatorios	Elementos secundarios opcionales
<cpix : >ContentK eyUsageRuleList	-	id	al menos un <cpix : >ContentK eyUsageRule	-
<cpix : >ContentK eyUsageRule	niño, intendedT rackType	-	al menos un <cpix: AudioFilt er > o un <cpix : >(*) VideoFilter	<cpix : >KeyPeriodFilter
<cpix : >KeyPeriodFilter	ID de período	-	-	-
<cpix : >AudioFil ter	-	minChannels, maxChannels	-	-
<cpix : >VideoFil ter	-	minPixels, maxPixels, hdr, minFps, maxFps	-	-

(*) Para obtener una explicación detallada sobre el uso de claves de contenido únicas o múltiples para proteger una o varias pistas de un streamset, consulte la sección de documentación del Contrato de cifrado._

SPEKE API v2: contrato de cifrado

El contrato de cifrado define qué claves de contenido protegen a qué pistas dentro de un conjunto de streamset determinado, en función de las características de las pistas.

El uso de varias claves de contenido para diferentes pistas de un streamset, a pesar de ser una práctica recomendada en el sector, no es obligatorio, pero sí recomendable: al menos dos claves de contenido diferentes, una para las pistas de audio y otra para las pistas de vídeo. Es posible utilizar una única clave de contenido para cifrar varias pistas, pero debe indicarse de forma explícita en el documento CPIX que el encriptador envía al proveedor de la clave. En términos generales,

el encriptador siempre describe con precisión cuántas claves de contenido se necesitan y cómo se aprovechan para cifrar las distintas pistas multimedia.

Principios

El contrato de cifrado se encuentra en la sección `<cpix:ContentKeyUsageRuleList>` del documento CPIX. En esta sección, cada clave de contenido definida en la sección `<cpix:ContentKeyList>` corresponde a un elemento `<cpix:ContentKeyUsageRule>` específico, que incluirá lo siguiente:

- un atributo `ContentKeyUsageRule@intendedTrackType` que puede hacer referencia a uno o más subcomponentes, separados por el signo “+” si se utilizan varios subcomponentes. El valor de `ContentKeyUsageRule@intendedTrackType` será único en un contrato de cifrado y no podrá utilizarse en varios elementos `ContentKeyUsageRule`.
- uno o más elementos secundarios `<cpix:AudioFilter>` o `<cpix:VideoFilter>`, según el valor del atributo `ContentKeyUsageRule@intendedTrackType`.

Las reglas que rigen esta relación son las siguientes:

- Si todas las pistas de audio y vídeo del streamset deben protegerse con una clave de contenido única, la cadena `'ALL'` debe utilizarse como valor de atributo `ContentKeyUsageRule@intendedTrackType`. El ejemplo 1 muestra un caso de uso de este tipo. En esta situación, deberán incluirse los elementos secundarios `<cpix:AudioFilter />` y `<cpix:VideoFilter />` sin ningún atributo. No es válida en este contexto concreto ninguna otra combinación de elementos `<cpix:AudioFilter>` y `<cpix:VideoFilter>`.
- Para todos los demás casos de uso, el valor del atributo `ContentKeyUsageRule@intendedTrackType` se puede definir libremente y el número de elementos secundarios `<cpix:AudioFilter />` y `<cpix:VideoFilter />` deben corresponder al número de subcomponentes agregados mediante el signo “+”. Los ejemplos 2/3/4/5/6/7/9/10 ilustran este requisito cuando un único subcomponente está presente en el valor del atributo `ContentKeyUsageRule@intendedTrackType`. El ejemplo 8 lo ilustra cuando se utilizan varios subcomponentes: `ContentKeyUsageRule@intendedTrackType="SD+HD"` se describe mediante dos elementos secundarios `<cpix:VideoFilter>` distintos con valores de atributos diferentes y `ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"` se describe mediante tres elementos secundarios `<cpix:VideoFilter>` distintos con valores de atributos diferentes.

Filtros

El CPIX define varios elementos y atributos de filtrado, pero SPEKE solo admite un subconjunto de ellos. Se resumen en la siguiente tabla:

Tipo de filtro CPIX	Soporte general de SPEKE	Los atributos de filtro son compatibles con SPEKE	Los atributos de filtro no son compatibles con SPEKE
<cpix : >VideoFilter	Sí	minPixels, maxPixels , hdr, minFps, maxFps (atributos opcionales)	wcg
<cpix : >AudioFilter	Sí	minChannels, maxChannels (atributos opcionales)	
<cpix : >KeyPerio dFilter	Sí	ID del período (atributo obligatorio)	
<cpix : >BitrateFilter	No	N/A	N/A
<cpix : >LabelFilter	No	N/A	N/A

Según la especificación del CPIX para VideoFilter, [minPixels, maxPixels] es un rango completo en ambas dimensiones, mientras que (minFps, maxFps] es inclusivo solo para la dimensión maxFps. Pues AudioFilter, [minChannels, maxChannels] es un rango inclusivo en ambas dimensiones.

Situaciones problemáticas

Hay situaciones en las que la información proporcionada en el contrato de cifrado puede ser parcial, ambigua o errónea. En estos casos, es importante que el encriptador y el proveedor de claves actúen de forma adecuada y garanticen una protección adecuada del contenido. En la siguiente tabla se presenta el comportamiento recomendado en estas situaciones:

En esta situación	El encriptador debería/deberá...	El proveedor de claves debería/deberá...
No se aplica ninguna regla a una o más pistas del streamset (consulte el ejemplo 3 a continuación)	El encriptador debe analizar su configuración (externa a la carga del CPIX) y comprobar que las pistas en cuestión no requieren cifrado. Si no es lo esperado, el encriptador debería generar un error y detener el procesamiento.	No es relevante: el proveedor de claves no conoce la estructura del streamset.
Varias reglas se superponen y sugieren múltiples claves de contenido para cifrar una pista específica	El cifrador debe aplicar lo último que se haya evaluado ContentKeyUsageRule correctamente en el orden del documento.	No es relevante: el proveedor de claves no conoce la estructura del streamset.
El contrato de cifrado cambia en un único ciclo de solicitud/respuesta de SPEKE	El encriptador establecerá una excepción y detendrá el procesamiento, ya que el proveedor de claves no es responsable de definir el contrato de cifrado.	Para evitar que se produzca esta situación, el proveedor de claves no debe modificar un contrato de cifrado recibido en la carga del CPIX de la solicitud SPEKE.
Contrato de cifrado mal formado: intendedTrackType / Filters, excepción de restricción de cardinalidad, filtros o atributos no compatibles	El encriptador deberá establecer una excepción, detener el procesamiento y no enviar la solicitud SPEKE al proveedor de claves, ya que lo más probable es que la protección del contenido sea errónea o que algunas pistas queden desprotegidas.	El proveedor de claves emitirá una excepción y devolverá un error de “Malformed encryption contract” (contrato de cifrado incorrecto).
Contrato de cifrado bien estructurado, pero que infringe	Si el encriptador conoce las limitaciones de los niveles de	El proveedor de claves establecerá una excepción y

En esta situación	El encriptador debería/deberá...	El proveedor de claves debería/deberá...
las restricciones de los niveles de seguridad del DRM: por ejemplo, se solicita una clave de contenido única para proteger tanto las pistas de audio como las pistas de vídeo UHD	seguridad del DRM, debería establecer una excepción, detener el procesamiento y no enviar la solicitud SPEKE al proveedor de claves, ya que lo más probable es que se traduzca en una protección del contenido errónea.	devolverá el mensaje de error “Requested CPIX encryptio n contract not supported” (El contrato de cifrado CPIX solicitado no es compatible).
Contrato de cifrado faltante	El cifrador no enviará documentos CPIX que no contengan ningún elemento o elemento. VideoFilter AudioFilt er	El proveedor de claves realizará una excepción y devolverá el mensaje de error “Missing CPIX encryption contract” (Falta el contrato de cifrado CPIX).

Ejemplos de contratos de cifrado

Ejemplo 1: una clave de contenido para todas las pistas de audio y vídeo

```
<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>
```

Ejemplo 2: una clave de contenido para todas las pistas de vídeo y una clave de contenido para todas las pistas de 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>
```

Ejemplo 3: una clave de contenido para todas las pistas de vídeo y pistas de audio sin cifrar

```
<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>
```

Ejemplo 4: varias claves de contenido para diferentes pistas de vídeo (SD/HD), una clave de contenido para todas las pistas de 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>
```

Ejemplo 5: múltiples claves de contenido para diferentes pistas de vídeo (SD/HD/UHD), una clave de contenido para todas las pistas de 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>
```

Ejemplo 6: varias claves de contenido para diferentes pistas de vídeo (SD/HD/UHD1/UHD2), una clave de contenido para todas las pistas de 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>
```

Ejemplo 7: varias claves de contenido para diferentes pistas de vídeo (SD/HD1/HD2/UHD1/UHD2), una clave de contenido para todas las pistas de 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>
```

Ejemplo 8: varias claves de contenido para diferentes pistas de vídeo (basadas en varios tipos de atributos), una clave de contenido para todas las pistas de 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>
```

Ejemplo 9: una clave de contenido para todas las pistas de vídeo y varias claves de contenido para las pistas de audio estéreo y audio multicanal

```
<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>
```

Ejemplo 10: una clave de contenido para todas las pistas de vídeo, varias claves de contenido para audio estéreo y dos tipos de pistas de audio multicanal

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

```
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for stereo audio tracks-->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
 </cpix:ContentKeyUsageRule>
 <!-- Rule for multichannel audio tracks (3 to 6 channels)-->
 <cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
 intendedTrackType="MULTICHANNEL_AUDIO_3_6">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="3" maxChannels="6"/>
 </cpix:ContentKeyUsageRule>
  <!-- Rule for multichannel audio tracks (7 channels and more)-->
 <cpix:ContentKeyUsageRule kid="81eb3761-55ff-4d22-a31d-94f01bbfd8ba"
 intendedTrackType="MULTICHANNEL_AUDIO_7">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="7"/>
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

SPEKE API v2: ejemplos de llamadas al método de flujo de trabajo en directo

Ejemplo de la sintaxis de la solicitud

La siguiente URL es un ejemplo y no indica un formato fijo:

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

Cuerpo de la solicitud

Un documento CPIX.

Encabezados de la solicitud

Nombre	Tipo	Se ejecuta	Descripción
`AWS Authorization`	Cadena	1..1	Consulte AWS Sigv4

Nombre	Tipo	Se ejecuta	Descripción
`X-Amz-Security-Token`	Cadena	1..1	Consulte AWS Sigv4
`X-Amz-Date`	Cadena	1..1	Consulte AWS Sigv4
`Content-Type`	Cadena	1..1	application/xml
`X-Speke-Version`	Cadena	1..1	Versión de la API SPEKE utilizada con la solicitud, formulada como MajorVersion. MinorVersion, como '2.0' para SPEKE v2.0

Encabezados de la respuesta

Nombre	Tipo	Se ejecuta	Descripción
`X-Speke-User-Agent`	Cadena	1..1	Cadena que identifica al proveedor de claves
`Content-Type`	Cadena	1..1	application/xml
`X-Speke-Version`	Cadena	1..1	Versión de la API SPEKE utilizada con la solicitud, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Respuesta a la solicitud

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	Respuesta de la carga de DASH-CPIX
`4XX (Client error)`	Mensaje de error del cliente	1..1	Descripción del error del cliente
`5XX (Server error)`	Mensaje de error del servidor	1..1	Descripción del error del servidor

> **Note**
>
> Los ejemplos que aparecen en esta sección no incluyen el cifrado de las claves de contenido. Para obtener información acerca de cómo agregar el cifrado de claves de contenido, consulte Cifrado de claves de contenido.

Carga de solicitud de ejemplo en directo con claves sin cifrar

En el siguiente ejemplo, se muestra una carga típica de solicitudes en directo desde el encriptador hasta el proveedor de claves DRM, con una clave de contenido para todas las pistas de vídeo y otra clave de contenido para todas las pistas de 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>
```

Carga de respuesta de ejemplo en directo con claves sin cifrar

En el siguiente ejemplo, se muestra una carga de respuesta típica del proveedor de claves DRM (los valores devueltos se han abreviado con [...] para facilitar la lectura):

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>h3toSFIlyAYpfXVQ795m6x==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
```

```
    <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
    <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
   </cpix:DRMSystem>
   <!-- Widevine -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
   </cpix:DRMSystem>
   <!-- Playready -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
```

```
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2: ejemplos de llamadas de método de flujo de trabajo de VOD

Ejemplo de la sintaxis de la solicitud

La siguiente URL es un ejemplo y no indica un formato fijo.

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

Cuerpo de la solicitud

Un documento CPIX.

Encabezados de la solicitud

Nombre	Tipo	Se ejecuta	Descripción
`AWS Authorization`	Cadena	1..1	Consulte AWS Sigv4
`X-Amz-Security-Token`	Cadena	1..1	Consulte AWS Sigv4

Nombre	Tipo	Se ejecuta	Descripción
`X-Amz-Date`	Cadena	1..1	Consulte AWS Sigv4
`Content-Type`	Cadena	1..1	application/xml
`X-Speke-Version`	Cadena	1..1	Versión de la API SPEKE utilizada con la solicitud, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Encabezados de la respuesta

Nombre	Tipo	Se ejecuta	Descripción
`X-Speke-User-Agent`	Cadena	1..1	Cadena que identifica al proveedor de claves
`Content-Type`	Cadena	1..1	application/xml
`X-Speke-Version`	Cadena	1..1	Versión de la API SPEKE utilizada con la solicitud, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Respuesta a la solicitud

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	Respuesta de la carga de DASH-CPIX

CÓDIGO HTTP	Nombre de la carga	Se ejecuta	Descripción
`4XX (Client error)`	Mensaje de error del cliente	1..1	Descripción del error del cliente
`5XX (Server error)`	Mensaje de error del servidor	1..1	Descripción del error del servidor

> **Note**
>
> Los ejemplos que aparecen en esta sección no incluyen el cifrado de las claves de contenido. Para obtener información acerca de cómo agregar el cifrado de claves de contenido, consulte Cifrado de claves de contenido.

Carga de solicitud de ejemplo de VOD con claves sin cifrar

En el siguiente ejemplo, se muestra una carga típica de una solicitud de VOD desde el encriptador hasta el proveedor de claves DRM, con una clave de contenido para todas las pistas de vídeo y otra clave de contenido para todas las pistas de 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>
```

Carga de respuesta de ejemplo de VOD con claves sin cifrar

En el siguiente ejemplo, se muestra una carga de respuesta típica del proveedor de claves DRM (los valores devueltos se han abreviado con [...] para facilitar la lectura):

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

```
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
   </cpix:DRMSystem>
   <!-- Playready -->
   <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
   <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyUsageRuleList>
   <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="VIDEO">
    <cpix:VideoFilter />
   </cpix:ContentKeyUsageRule>
   <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  intendedTrackType="AUDIO">
    <cpix:AudioFilter />
   </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
```

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

SPEKE API v2: cifrado de claves de contenido

Si lo desea, puede añadir el cifrado de claves de contenido en la implementación de SPEKE. El cifrado de claves de contenido garantiza una end-to-end protección total al cifrar las claves de contenido para su tránsito, además de cifrar el contenido en sí. Si no implementa esta funcionalidad para su proveedor de claves, debe utilizar el cifrado de capa de transporte junto con un sólido mecanismo de autenticación para garantizar la seguridad.

Para utilizar el cifrado de claves de contenido para los cifradores que se ejecutan en la nube de AWS, los clientes importan los certificados al AWS Certificate Manager y, a continuación, utilizan el certificado resultante ARNs para sus actividades de cifrado. El cifrador utiliza el certificado ARNs y el servicio ACM para proporcionar claves de contenido cifrado al proveedor de claves DRM.

Restricciones

SPEKE admite el cifrado de claves de contenido tal y como se establece en la especificación DASH-IF CPIX con las siguientes restricciones:

- SPEKE no admite la verificación de firma digital (XMLDSIG) para cargas de solicitud o respuesta.
- SPEKE requiere 2048 certificados basados en RSA.

Estas restricciones también se enumeran en Personalizaciones y restricciones a la especificación DASH-IF.

Implementación del cifrado de claves de contenido

Para proporcionar el cifrado de claves de contenido, haga lo siguiente en las implementaciones del proveedor de claves de DRM:

- Administre el elemento `<cpix:DeliveryDataList>` en las cargas de las solicitudes y las respuestas.
- Proporcione valores cifrados en el elemento `<cpix:ContentKeyList>` de las cargas de respuesta.

Para obtener más información sobre estos elementos, consulte la especificación DASH-IF CPIX 2.3.

Ejemplo del elemento `<cpix:DeliveryDataList>` de cifrado de claves de contenido en la carga de una solicitud

```
<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>
```

Ejemplo del elemento `<cpix:DeliveryDataList>` de cifrado de claves de contenido en la carga de una respuesta

```
<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>
```

Ejemplo del elemento `<cpix:ContentKeyList>` de cifrado de claves de contenido en la carga de una respuesta

En el ejemplo siguiente se muestra la gestión de las claves de contenido cifradas en el elemento `<cpix:ContentKeyList>` de la carga de respuesta. Aquí se utiliza el 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>
```

En comparación, el siguiente ejemplo muestra una carga de respuesta similar con la clave de contenido entregada sin cifrar, como una clave sin cifrar. Aquí se utiliza el elemento `<pskc:PlainValue>`:

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

SPEKE API v2: anulación del identificador clave

El encriptador crea un nuevo identificador de clave (KID) cada vez que se modifican las claves. A continuación, pasa el KID al servidor de claves de DRM en las solicitudes. Casi siempre, el servidor de claves responde utilizando el mismo KID, aunque puede proporcionar un valor de KID diferente en la respuesta.

A continuación, se muestra un ejemplo de una solicitud con el 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 siguiente respuesta invalida el KID por `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>
```

Licencia para la especificación de la API SPEKE

Licencia pública internacional Creative Commons Attribution- ShareAlike 4.0

Al ejercer los derechos de licencia (definidos a continuación), usted acepta y acepta regirse por los términos y condiciones de esta licencia pública internacional Creative Commons Attribution ShareAlike 4.0 («Licencia pública»). En la medida en que esta licencia pública se puede interpretar como un contrato, a usted se le conceden derechos con licencia teniendo en cuenta su aceptación de estos términos y condiciones, y el licenciante le concede dichos derechos en consideración de las ventajas que el licenciante recibe de hacer material con licencia esté disponible conforme a estos términos y condiciones.

Sección 1. Definiciones.

a. El material adaptado se refiere al material sujeto a derechos de copyright y similares derivado del material con licencia, o basados en él, y en el que el material con licencia se traduce, altera, organiza, transforma o modifica de otra manera de una forma que requiere permiso en virtud de

los derechos de copyright y similares mantenidos por el licenciante. A los efectos de esta licencia pública, donde el material con licencia es una obra musical, actuación o grabación de sonido, el material adaptado siempre se produce donde el material con licencia está sincronizado en relación sincronizada con una imagen en movimiento.

b. La licencia del adaptador se refiere a la licencia que usted aplica a sus derechos de copyright y similares en sus contribuciones al material adaptado de acuerdo con los términos y condiciones de la presente licencia pública.

c. Por licencia compatible con BY-SA se entiende una licencia que aparece en creativecommons.org/compatiblelicenses y que ha sido aprobada por Creative Commons básicamente como el equivalente de esta licencia pública.

d. Los derechos de copyright y similares se refieren a los derechos de autor (copyright) y/o derechos similares estrechamente relacionados con los derechos de autor (copyright), lo que incluye, a título enunciativo, actuaciones, difusiones, grabaciones de sonido y derechos sui generis sobre bases de datos, sin tener en cuenta la forma en que los derechos se etiquetan o clasifican. A los efectos de la presente licencia pública, los derechos especificados en la sección 2(b) (1)-(2) no tienen derechos de copyright y similares.

e. Se denomina medidas tecnológicas eficaces a las medidas que, en ausencia de la autoridad adecuada, no se pueden eludir conforme a las leyes que cumplen las obligaciones en virtud del artículo 11 del Tratado de la OMPI sobre derechos de autor adoptado el 20 de diciembre de 1996 y/o acuerdos internacionales similares.

f. Excepciones y limitaciones indica el uso justo, trato justo y/o cualquier otra excepción o limitación de derechos de copyright y similares que se aplica a su uso del material con licencia.

g. Por elementos de licencia se entiende los atributos de licencia que figuran en el nombre de una licencia pública de Creative Commons. Los elementos de licencia de esta licencia pública son la atribución y. ShareAlike

h. Material con licencia es el trabajo artístico o literario, la base de datos u otro material sobre el que el Licenciante ha aplicado esta Licencia pública.

i. Derechos con licencia indica los derechos que se le conceden a usted sujetos a los términos y condiciones de la presente licencia pública, que se limitan a todos derechos de copyright y similares que se aplican a su uso del material con licencia y que el licenciante tiene autoridad para autorizar bajo licencia.

j. Licenciante es/son la(s) persona(s) o entidad(es) que concede(n) derechos en virtud de la presente licencia pública.

k. Compartir significa proporcionar material al público por cualquier medio o proceso que requiera permiso en virtud de los derechos con licencia, como la reproducción, exhibición pública, distribución, difusión, comunicación o importación, y poner el material a disposición del público, incluso de maneras en que personas del público pueden acceder al material desde un lugar y en un momento elegido de manera individual por ellos.

l. Derechos sui generis sobre bases de datos son los derechos distintos de los derechos de autor (copyright) resultado de la Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996 sobre la protección jurídica de las bases de datos, en su forma enmendada y/o reemplazada, así como otros derechos esencialmente equivalentes en cualquier lugar del mundo.

m. Usted se refiere a la persona o entidad que ejerce los derechos con licencia en virtud de la presente licencia pública. Usted tiene un significado pertinente.

Sección 2. Ámbito.

a. Concesión de licencia.

1. Sujeto a los términos y condiciones de la presente licencia pública, el licenciante le concede a usted por la presente una licencia mundial, libre de regalías, no sublicenciable, no exclusiva e irrevocable para ejercer los derechos con licencia en el material con licencia para:

   A. Reproducir y compartir el material con licencia, en su totalidad o en parte; y

   B. Producir, reproducir y compartir el material adaptado.

2. Excepciones y limitaciones. Para evitar dudas, donde se aplican excepciones y limitaciones a su uso, no se aplica la presente licencia pública y usted no tiene que cumplir con sus términos y condiciones.

3. Período. El plazo de la presente licencia pública se especifica en la sección 6(a).

4. Soportes y formatos; se permiten modificaciones técnicas. El licenciante autoriza a usted a ejercer los derechos con licencia en todos los soportes y formatos, ya sean conocidos ahora o se creen en adelante, y a realizar modificaciones técnicas necesarias para ello. El licenciante renuncia y/o acuerda no hacer valer ningún derecho o autoridad para prohibirle a usted realizar las modificaciones técnicas necesarias para ejercer los derechos con licencia, incluidas las modificaciones técnicas necesarias para eludir las medidas tecnológicas efectivas. A los efectos de la presente licencia pública, la simple realización de modificaciones autorizadas por esta sección 2(a)(4) nunca produce el material adaptado.

5. Destinatarios posteriores.

A. Oferta del licenciante: material con licencia. Todos los destinatarios del material con licencia reciben automáticamente una oferta del licenciante para ejercer los derechos con licencia en virtud de los términos y condiciones de esta licencia pública.

B. Oferta adicional del licenciante: material adaptado. Cada destinatario de su material adaptado recibirá automáticamente una oferta del licenciante para ejercer los derechos licenciados sobre el material adaptado según las condiciones de la licencia de adaptador que usted solicite.

C. Sin restricción posterior. No puede ofrecer ni imponer ningún término o condición diferente o adicional, ni aplicar ninguna de las medidas tecnológicas efectivas al material con licencia si al hacerlo se restringe el ejercicio de los derechos con licencia por parte de cualquier destinatario del material con licencia.

6. Sin endoso. Nada de la presente licencia pública constituye o puede considerarse un permiso para afirmar o implicar que usted, o que el uso que realice del material con licencia, están conectados con, patrocinados, endosados o se le ha concedido un carácter oficial por, el licenciante u otros designados para recibir la atribución según se estipula en la sección 3(a)(1)(A)(i).

b. Otros derechos.

1. Los derechos morales, como el derecho a la integridad, no están autorizados en virtud de esta Licencia Pública, ni tampoco la publicidad o la privacidad. Se and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or compromete a no hacer valer ninguno de esos derechos del licenciante en la medida necesaria para permitirle ejercer los derechos licenciados, pero no de otra manera.
2. Los derechos de patentes y de marca comercial no están autorizados en virtud de la presente licencia pública.
3. En la medida de lo posible, el licenciante renuncia a cualquier derecho de recopilar regalías de usted para el ejercicio de los derechos con licencia, ya sea directamente o a través de un organismo de recaudación, en virtud de cualquier esquema de licencias normativo u obligatorio voluntario o renunciable. En todos los demás casos, el licenciante se reserva expresamente cualquier derecho de recopilar dichas regalías.

Sección 3. Condiciones de la licencia.

Su ejercicio de los derechos con licencia está sujeto de manera expresa a que se cumplan las siguientes condiciones.

a. Atribución.

1. Si usted decide compartir el material con licencia (incluido en la forma modificada), debe:

   A. Conservar lo siguiente si se suministra por el licenciante con el material con licencia:

```
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. Indicar si usted ha modificado el material con licencia y conservar una indicación de las modificaciones anteriores; e

   C. Indicar que el material con licencia está autorizado en virtud de la licencia pública e incluir el texto de la presente licencia pública, o la URL o el hipervínculo para ella.

2. Puede satisfacer las condiciones de la sección 3(a)(1) de cualquier manera razonable en función de los soportes, medios y contextos en los que usted decida compartir el material con licencia. Por ejemplo, puede ser razonable satisfacer las condiciones proporcionando una URL o hipervínculo a un recurso que incluya la información necesaria.

3. Si se lo solicita el licenciante, usted debe eliminar cualquier información requerida por la sección 3(a)(1)(A) en la medida de lo razonablemente posible.

b. ShareAlike. Además de las condiciones de la sección 3 (a), si compartes material adaptado que produzcas, también se aplicarán las siguientes condiciones.

1. La licencia del adaptador que solicite debe ser una licencia de Creative Commons con los mismos elementos de licencia, en esta versión o posterior, o una licencia compatible con BY-SA.

2. Debe incluir el texto, la URL o el hipervínculo de la licencia del adaptador que solicite. Puede cumplir con esta condición de cualquier manera razonable en función de los soportes, medios y contextos en los que usted decida compartir el material adaptado.

3. No puede ofrecer ni imponer términos o condiciones adicionales o diferentes, ni aplicar ninguna medida tecnológica efectiva al material adaptado que restrinja el ejercicio de los derechos otorgados en virtud de la licencia del adaptador que solicite.

Sección 4. Derechos sui generis sobre bases de datos.

Cuando los derechos con licencia incluyan derechos sui generis sobre bases de datos que se apliquen a su uso del Material con licencia:

a. Para evitar dudas, la sección 2(a)(1) le concede a usted el derecho de extraer, reutilizar, reproducir y compartir todo el contenido de la base de datos o una parte importante de dicho contenido;

b. si usted incluye todo el contenido de la base de datos o una parte importante de dicho contenido en una base de datos en la que usted tiene derechos sui generis sobre bases de datos, la base de datos en la que tienen dichos derechos (pero no su contenido individual), es material adaptado, se incluye a los efectos en la sección 3(b); y

c. debe cumplir las condiciones de la sección 3(a) si usted decide compartir todo el contenido de la base de datos o una parte importante de dicho contenido. Para evitar dudas, esta sección 4 es un suplemento y no reemplaza sus obligaciones en virtud de la presente licencia pública donde los derechos con licencia incluyen otros derechos de copyright y similares.

Sección 5. Exención de garantías y limitación de responsabilidad.

a. A menos que se aborde de otra manera por separado por el licenciante, en la medida de lo posible, el licenciante ofrece el material con licencia como tal y según está disponible y no genera ninguna declaración ni garantía de ningún tipo relativa al material con licencia, ya sea expresa, implícita, normativa o de otro tipo. Esto incluye, sin limitación, garantías de título, comerciabilidad, idoneidad para un determinado fin, no infracción, ausencia de vicios ocultos u otros defectos, precisión o la presencia o ausencia de errores, ya sean o no conocidos o detectables. Donde no se permiten las renuncias de garantías en su totalidad o en parte, esta renuncia no es aplicable para usted.

b. En la medida de lo posible, en ningún caso el licenciante será responsable ante usted de cualquier teoría legal (lo que incluye, sin que sirva de limitación) o de otra manera de ningún daño directo, especial, indirecto, incidental, consecuente, punitivo, ejemplar, o de otras pérdidas, costos, gastos o daños que surjan de la presente licencia pública o del uso del material con licencia, incluso si se ha advertido al licenciante de la posibilidad de dichas pérdidas, costos, gastos o daños. Donde

no se permita una limitación de responsabilidad en su totalidad o en parte, es posible que esta limitación no sea aplicable para usted.

c. La renuncia de garantías y la limitación de responsabilidad proporcionada anteriormente se interpretará de modo que, en la medida de lo posible, se aproxime más a una renuncia absoluta y una exoneración de toda responsabilidad.

Sección 6. Plazo y finalización.

a. Esta licencia pública se aplica durante el plazo de los derechos de copyright y similares autorizados aquí. Sin embargo, si usted no cumple con la presente Licencia pública, sus derechos en virtud de esta Licencia pública finalizarán automáticamente.

b. Cuando su derecho de utilizar el material con licencia haya finalizado en virtud de la sección 6(a), se reinstaura:

   1. automáticamente desde la fecha en que se subsana la infracción, siempre que se subsane en un plazo de 30 días a partir de la detección de la infracción; o

   2. tras la restauración expresa por parte del licenciante.

c. Para evitar dudas, esta sección 6(b) no afecta a ningún derecho que el licenciante pueda tener para buscar soluciones para sus infracciones de la presente licencia pública.

d. Para evitar dudas, el licenciante también puede ofrecer el material con licencia según otros términos o condiciones o dejar de distribuir el Material con licencia en cualquier momento; sin embargo, esto no pondrá fin a la presente licencia pública.

e. Las secciones 1, 5, 6, 7 y 8 seguirán vigentes tras la finalización de la presente licencia pública.

Sección 7. Otros términos y condiciones.

a. El licenciante no estará vinculado a ningún término o condición adicional o diferente comunicado por usted a menos que se acuerde de manera expresa.

b. Los arreglos, entendimientos o acuerdos referentes al material con licencia no mencionados en el presente documento están separados de los términos y condiciones de la presente Licencia pública y son independientes de ellos.

Sección 8. Interpretación.

a. Para evitar dudas, la presente licencia pública no reduce, limita, restringe ni impone condiciones, ni se interpretará como tal, sobre cualquier uso del material con licencia que podría realizarse legalmente sin permiso en virtud de la presente licencia pública.
b. En la medida de lo posible, si alguna disposición de la presente licencia pública se considera inejecutable, se reformará en la mínima medida necesaria para que sea aplicable. Si la disposición no se puede reformar, se separará de la presente licencia pública sin afectar a la aplicabilidad del resto de términos y condiciones.
c. No se renunciará a ningún término o condición de la presente licencia pública y no se consentirá su incumplimiento a menos que el licenciante lo acuerde de manera expresa.
d. Nada de la presente licencia pública constituye o se puede interpretar como una limitación, o renuncia, de los privilegios e inmunidades que se aplican al licenciante o a usted, incluidos desde los procesos legales de cualquier jurisdicción o autoridad.

Historial de documentos de la guía para socios y clientes de SPEKE

En la siguiente tabla se describen los cambios en la documentación de SPEKE.

SPEKE v1

Cambio	Descripción	Fecha
Matriz de compatibilidad: servicios y productos de socios de AWS	Se agregó una nueva sección para soporte SPEKE en los servicios y productos de los socios de AWS, con una lista de los servicios de Bitmovin.	13 de enero de 2023
Actualizaciones de proveedor es de plataforma DRM	Se han añadido enlaces e información de socios nueva a la lista de proveedores de la plataforma DRM.	24 de enero de 2019
Incluir encriptadores de terceros	Se ha actualizado la arquitect ura y las descripciones para considerar los encriptadores de terceros.	20 de noviembre de 2018
Cifrado de las claves de contenido	Se ha agregado la opción de cifrar las claves de contenido . Anteriormente, Secure Packager and Encoder Key Exchange solo admitía la entrega de claves sin cifrado.	30 de octubre de 2018
Matriz de compatibilidad: AWS Elemental Live	Se ha añadido una matriz de compatibilidad de AWS Elemental Live.	27 de septiembre de 2018
Componentes de carga estándares	Se ha añadido una sección en la que se definen los principal	27 de septiembre de 2018

Cambio	Descripción	Fecha
	es elementos de la carga JSON.	
Invalidación de KID	Se ha añadido una sección sobre la invalidación de KID realizada por un proveedor de claves.	27 de septiembre de 2018
Se han corregido los enlaces al sitio de DASH-IF.	Se corrigieron los enlaces al sitio de DASH IF para ver la especificación del CPIX y la página del sistema. IDs	27 de septiembre de 2018
Facilitar copia de la versión de AWS Elemental Live	Se ha actualizado la documentación de SPEKE para incluir productos de AWS Elemental.	20 de julio de 2018
CMAF	Se han actualizado las tablas de las matrices de compatibi lidad para incluir el formato común de aplicaciones multimedia (CMAF).	27 de junio de 2018
Versión inicial	Lanzamiento inicial de la versión 1 de SPEKE, una especificación para las comunicaciones entre un encriptador de contenido y un proveedor de claves de DRM. El proveedor de claves de DRM presenta una API de SPEKE para gestionar las solicitudes de claves entrantes .	27 de noviembre de 2017

SPEKE v2

Cambio	Descripción	Fecha
Actualizaciones de la sección de proveedores de plataform as DRM y de la sección de servicios y productos de AWS compatibles con SPEKE	Se agregó Webstream a la columna SPEKE v2 de la lista de proveedores de plataformas DRM y se agregó MediaConvert a la columna SPEKE v2 de la tabla de soporte de SPEKE en los servicios y productos de AWS.	10 de octubre de 2024
Actualizaciones de la sección de proveedores de plataforma DRM	Se han añadido nuevos socios calificados a la columna SPEKE v2 de la lista de proveedores de plataformas DRM.	9 de agosto de 2023
Actualizaciones de las secciones de ejemplos de llamadas a métodos de flujo de trabajo en directo y VOD	Se agregó el encabezado de X-Speke-Version respuesta que faltaba en las secciones de ejemplos de llamadas a métodos de flujo de trabajo VOD y en directo de SPEKE v2.	13 de enero de 2023
Actualizaciones de los proveedores de plataform as DRM y de la sección de contratos de cifrado	Se han añadido nuevos socios calificados a la columna SPEKE v2 de la lista de proveedores de plataformas DRM. Se han añadido dos nuevos ejemplos de contratos de cifrado y se ha cambiado la resolución máxima de SD a 1024 x 576 en todos los ejemplos correspondientes.	27 de enero de 2022

Cambio	Descripción	Fecha
Lanzamiento inicial	Lanzamiento inicial de la versión 2.0 de SPEKE, una especificación para la comunicación entre un encriptador de contenido y un proveedor de claves de DRM. El proveedor de claves de DRM presenta una API de SPEKE para gestionar las solicitudes de claves entrantes .	7 de septiembre de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.