Guía para socios y clientes

Especificación de intercambio seguro de claves de empaquetador y codificador API

Especificación de intercambio seguro de claves de empaquetador y codificador API: Guía para socios y clientes

Table of Contents

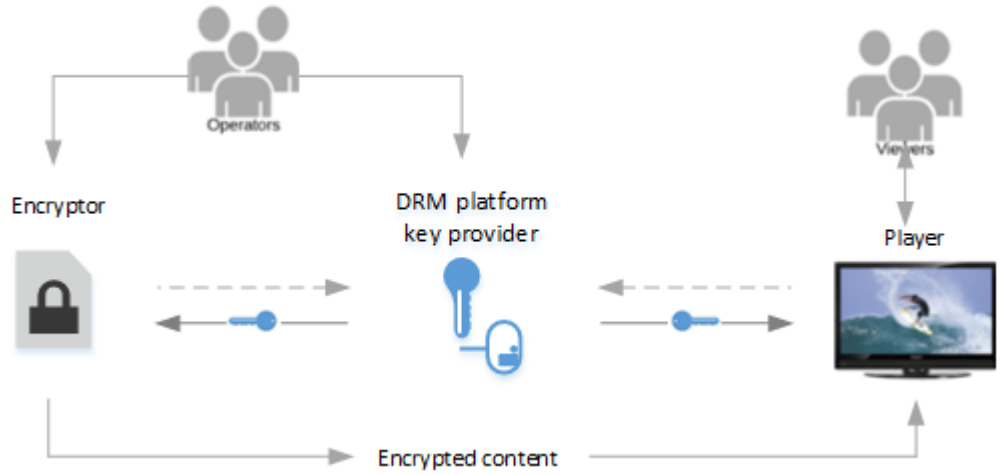
¿Qué es Secure Packager and Encoder Key Exchange?

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

Temas

Arquitectura general

La siguiente ilustración muestra una vista de alto nivel de la arquitectura de cifrado de SPEKE contenido para los productos locales.



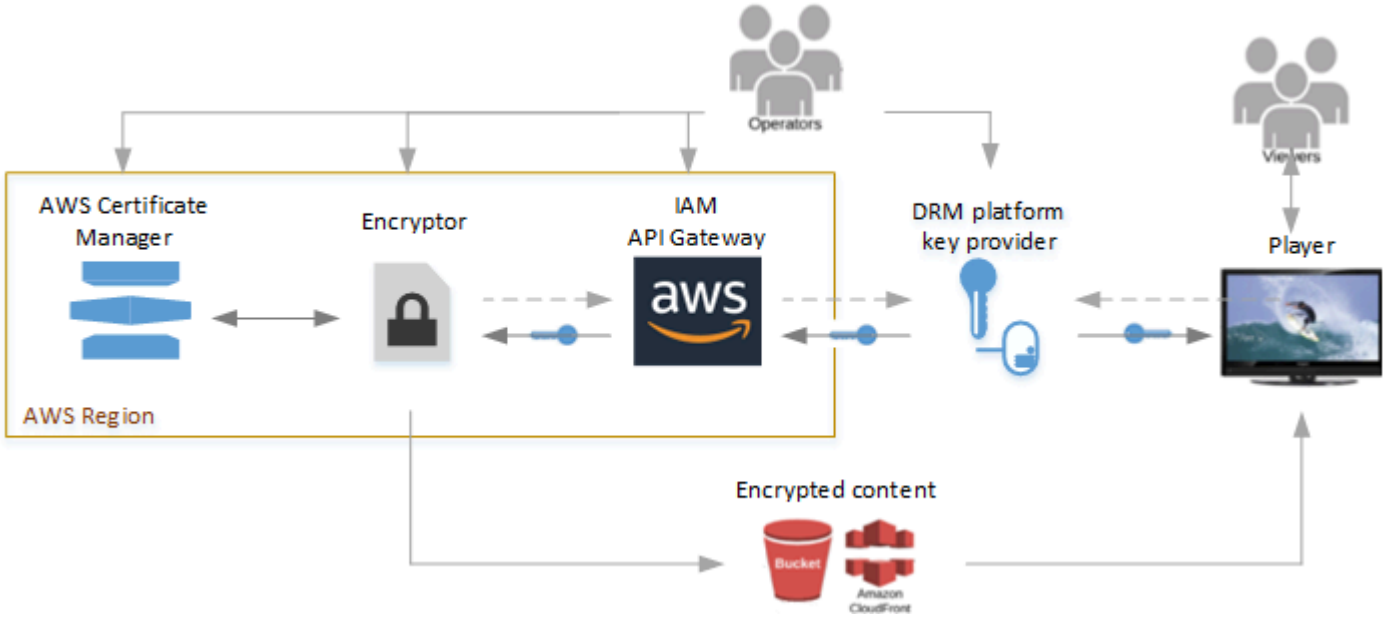
Estos son los principales componentes de la arquitectura anterior:

- Encriptador: proporciona la tecnología de cifrado. Recibe las solicitudes de cifrado de su operador y recupera las claves necesarias del DRM proveedor de claves para proteger el contenido cifrado.
- DRMproveedor de claves de plataforma: proporciona claves de cifrado al cifrador a través de un SPEKE sistema compatible. API El proveedor también proporciona licencias a los reproductores multimedia para que puedan descifrar el contenido.

- Reproductor: solicita las claves al mismo proveedor de claves de la DRM plataforma, que el reproductor utiliza para desbloquear el contenido y mostrárselo a sus espectadores.

AWSarquitectura basada en la nube

La siguiente ilustración muestra la arquitectura de alto nivel cuando SPEKE se usa con servicios y funciones que se ejecutan en la AWS nube.



Estos son los principales servicios y componentes:

- Encriptador: proporciona la tecnología de cifrado en la AWS nube. El cifrador recibe las solicitudes de su operador y recupera las claves de cifrado necesarias del DRM proveedor de claves, 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.
- AWSIAMy Amazon API Gateway: administra las funciones de confianza del cliente y la comunicación proxy entre el cifrador y el proveedor de claves. APIGateway ofrece funciones de registro y permite a los clientes controlar sus relaciones con el cifrador y con la plataforma. DRM Los clientes permiten el acceso de los proveedores de claves mediante la configuración de IAM roles. APILa puerta de enlace debe residir en la misma AWS región que el cifrador.
- AWSCertificate 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 residir en la misma AWS región que el cifrador.

- DRMproveedor de claves de plataforma: proporciona claves de cifrado al cifrador mediante un SPEKE sistema compatible. API El proveedor también proporciona licencias a los reproductores multimedia para que puedan descifrar el contenido.
- Reproductor: solicita las claves al mismo proveedor de claves de la DRM plataforma, que el reproductor utiliza para desbloquear el contenido y mostrárselo a sus espectadores.

Cómo comenzar

Para obtener material introductorio adicional sobre el SPEKE tema, consulta ¿Eres nuevo en estoSPEKE? .

¿Es cliente?

Asóciese con un proveedor de la DRM plataforma AWS Elemental para configurar el uso del cifrado. Para obtener más información, consulte Incorporación de clientes.

¿Eres un proveedor de DRM plataformas o un cliente con tu propio proveedor de claves?

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

¿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 introducciónSPEKE, vea el siguiente webcast:

Información y especificaciones del servicio relacionadas

- APIpermisos de puerta de enlace: cómo controlar el acceso a un API sistema con permisos de AWS Identity and Access Management (AWSIAM).
- AWS AssumeRole— Cómo utilizar AWS Security Token Service (AWSSTS) para asumir la funcionalidad del rol.
- AWSSigv4 — Cómo firmar una HTTP solicitud con Signature, versión 4.
- DASHEspecificación -IF v2.0: versión de CPIX especificación del formato de intercambio de información sobre protección de contenido (CPIX) DASH -IF, en la que se basa esta especificación SPEKE v1.0.
- DASHCPIX-Especificación IF v2.3: versión de especificación del formato de intercambio de información sobre protección de contenido (CPIX) DASH -IF, en la que se basa esta especificación v2.0. SPEKE
- DASH-Sistema 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 puedes usar con tu AWS cuenta y ayudarte a empezar con una SPEKE implementación 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 CPIXespecificación DASH -IF.

- ARN— Nombre del recurso de Amazon. Identifica un AWS recurso de forma única.
- 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 medios 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— Gestión de derechos digitales. Se utiliza para proteger el contenido digital protegido por derechos de autor frente a accesos sin autorización.
- DRMplataforma: sistema que proporciona DRM funcionalidad y soporte a los cifradores y espectadores de contenido, incluido el suministro de DRM claves y licencias para el cifrado y descifrado de contenido.
- DRMproveedor: consulte DRM la plataforma.
- DRMsistema: un estándar para DRM las implementaciones. DRMLos sistemas más comunes incluyen Apple FairPlay, Google Widevine y Microsoft. PlayReady DRMLos proveedores de contenido utilizan los sistemas para proteger el contenido digital para su entrega a los espectadores y para que los espectadores puedan acceder a él. Para obtener una lista de DRM los sistemas que están registrados en DASH -IF, consulte Sistema DASH-IF. IDs La CPIXespecificación DASH -IF usa el término «DRMsistema» tal como se define aquí y, en algunos lugares, usa «DRMsistema» para referirse a lo que esta especificación denomina plataforma. DRM
- DRMsolución: consulte la DRM plataforma.
- DRMtecnología: consulte DRM el sistema.
- Encriptador: un componente de procesamiento multimedia que cifra el contenido multimedia con claves obtenidas del proveedor de claves. Los cifradores también suelen añadir señalización de DRM cifrado y metadatos a los medios. Los encriptadores suelen ser codificadores, empaquetadores y transcodificadores.
- Proveedor de claves: el componente de una DRM plataforma que permite gestionar SPEKE REST API 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 DRM plataforma 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 su información de diferentes fuentes, incluidos los archivos de manifiesto multimedia, los archivos multimedia y DRM las licencias. Solicita licencias a la DRM plataforma en nombre de los espectadores.

Incorporación de clientes para SPEKE

Proteja su contenido del uso no autorizado combinando un proveedor de claves de administración de derechos digitales (SPEKE) de Secure Packager y Encoder Key Exchange (DRM) con su encriptador y sus reproductores multimedia. SPEKEdefine el estándar de comunicación entre los codificadores y empaquetadores de contenido multimedia y los proveedores de claves de gestión de derechos digitales (). DRM Para incorporarse, debe elegir un proveedor de claves de DRM plataforma y configurar la comunicación entre el proveedor de claves y sus codificadores y reproductores.

Temas

Comience con un proveedor de DRM plataformas

Los siguientes socios de Amazon proporcionan implementaciones de DRM plataformas de terceros paraSPEKE. 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.

DRMproveedor de plataformas	SPEKEsoporte v1	SPEKEsoporte v2
Axinom	√	√
Comprar DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKARedes	√	√
Nube Insys DRM	√	√

DRMproveedor de plataformas	SPEKEsoporte v1	SPEKEsoporte v2
Intertrust Technologies	√	√
Irdeto	√	√
JW Player	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKEsoporte en AWS servicios y productos

En esta sección se detalla el SPEKE soporte que ofrecen los servicios AWS multimedia que se ejecutan en la AWS nube y los productos multimedia AWS locales. Estos servicios y productos son los cifradores de la arquitectura de cifrado de SPEKE contenido. Compruebe que el protocolo de streaming y el DRM sistema que desea estén disponibles para su servicio o producto.

AWSservicio o producto	SPEKEsoporte v1	SPEKEsoporte v2	DRMTecnologías compatibles
AWSElemental MediaConvert : servicio que se ejecuta en la AWS nube	√	√	Documentación

AWSservicio o producto	SPEKEsoporte v1	SPEKEsoporte v2	DRMTecnologías compatibles
AWSElemental MediaPackage : servicio que se ejecuta en la AWS nube	√	√	Documentación
AWSElemental Live: producto local	√		Documentación: MPEG-/DASHHLS
AWSElemental Server: producto local	√		Documentación

SPEKEsoporte en los servicios y AWS productos de los socios

En esta sección se detalla el SPEKE soporte que ofrecen los servicios y productos de los AWS socios que se ejecutan en la AWS nube. Estos servicios y productos son los cifradores de la arquitectura de cifrado de SPEKE contenido. Compruebe que el protocolo de streaming y el DRM sistema que desea estén disponibles para su servicio o producto.

AWSservicio o producto	SPEKEsoporte v1	SPEKEsoporte v2	DRMTecnologías compatibles
Codificación de vídeo en directo con Bitmovin	√		Documentación
Codificación de vídeo bajo demanda en Bitmovin () VOD	√		Documentación

SPEKEAPIespecificación

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

En un flujo de trabajo de transmisión de vídeo, el motor de cifrado se comunica con el proveedor de claves de la DRM plataforma para solicitar las 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 lograr un end-to-end cifrado más seguro.

Esta especificación persigue los siguientes objetivos:

- Defina una interfaz sencilla, fiable y altamente segura que DRM los proveedores y los clientes puedan utilizar para integrarla con los cifradores cuando sea necesario cifrar el contenido.
- Cubra VOD y ejecute los flujos de trabajo e incluya las condiciones de error y los mecanismos de autenticación necesarios para una comunicación sólida y altamente segura entre los cifradores y los terminales de los proveedores de DRM claves.
- Incluya soporte para HLSMSS, DASH empaquetado y sus DRM sistemas comunes: FairPlay PlayReady, y Widevine/. CENC
- Mantenga la especificación simple y ampliable para soportar futuros DRM sistemas.
- Use un método simple RESTAPI.

> **Note**
>
>

ARISINGFROM, OUT DE O EN CONNECTION WITH THIS MATERIAL O EN THE USE O OTHER DEALINGS DE THISMATERIAL.

Temas

Se requiere autenticación para SPEKE

SPEKErequiere autenticación para los productos locales y para los servicios y funciones que se ejecutan en la AWS nube.

Temas

Autenticación para implementaciones AWS en la nube

SPEKErequiere AWS la autenticación mediante IAM funciones para su uso con un cifrador. IAMlos roles los crea el DRM proveedor o el operador propietario del DRM punto final de una AWS cuenta. A cada función se le asigna un nombre de recurso de Amazon (ARN), que el operador del servicio AWS Elemental proporciona en la consola de servicio al solicitar el cifrado. Los permisos de política del rol deben configurarse para permitir el acceso al proveedor de claves API y no el acceso a otros AWS recursos. Cuando el cifrador se pone en contacto con el proveedor de DRM claves, utiliza la función ARN para asumir la función de titular de la cuenta del proveedor de claves, que devuelve las credenciales temporales para que el cifrador las utilice para acceder al proveedor de claves.

Una implementación habitual consiste en que el operador o el proveedor de la DRM plataforma utilicen Amazon API Gateway delante del proveedor de claves y, a continuación, habiliten la autorización de AWS Identity and Access Management (AWSIAM) 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.

El siguiente ejemplo muestra un rol ARN que se crea para acceder al proveedor de DRM claves:

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

Para obtener más información sobre la creación de un rol, consulte AWS AssumeRole. Para obtener más información sobre la firma de una solicitud, consulte AWSSigv4.

Autenticación de productos en las instalaciones

En el caso de los productos locales, le recomendamos que utilice la autenticaciónSSL/TLSy la autenticación implícita para garantizar la máxima seguridad, pero como mínimo debería utilizar la autenticación básica en vez de la autenticación. HTTPS

Ambos tipos de autenticación utilizan el `Authorization` encabezado de la HTTP solicitud:

- Resumen de autenticación: el encabezado de autorización consta del identificador `Digest` seguido de una serie de valores que autentican la solicitud. En concreto, 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 información sobre la autenticación básica y resumida, incluida información detallada sobre el encabezado, consulte la especificación RFC2617 del Grupo de Trabajo de Ingeniería de Internet (IETF), titulada HTTP Autenticación: autenticación de acceso básica e implícita.

SPEKEAPIv1

Esta es la versión REST API 1 para Secure Packager and Encoder Key Exchange (SPEKE). Utilice esta especificación para proteger los DRM derechos de autor a los clientes que utilizan el cifrado. Para SPEKE cumplir con las normas, el proveedor de DRM claves debe exponer lo REST API descrito en esta especificación. El cifrador realiza API llamadas a su proveedor de claves.

> **Note**
>
> Los ejemplos de código de esta especificación se proporcionan únicamente con fines ilustrativos. No puede ejecutar los ejemplos porque no forman parte de una SPEKE implementación completa.

SPEKEutiliza la definición de estructura de datos del formato de intercambio de información sobre protección de contenido (DASH-IF-CPIX) del foro DASH industrial para el intercambio de claves, con algunas restricciones. DASH-IF- CPIX define un esquema para proporcionar un DRM intercambio múltiple y extensible desde la DRM plataforma 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 empaquetado de tasas de bits adaptables incluyenHLS, y. DASH MSS

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

Temas

- SPEKEAPIv1: Personalizaciones y restricciones de la especificación -IF DASH
- SPEKEAPIv1: componentes de carga útil estándar
- SPEKEAPIv1: ejemplos de llamadas a métodos de flujo de trabajo en vivo

- SPEKEAPIv1: ejemplos de llamadas a métodos VOD de flujo de trabajo
- SPEKEAPIv1: cifrado de claves de contenido
- SPEKEAPIv1 - Latido
- SPEKEAPIv1: anular el identificador clave

SPEKEAPIv1: Personalizaciones y restricciones de la especificación -IF DASH

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

- SPEKE sigue el flujo de trabajo Encriptador-Consumidor.
- Para las claves de contenido cifradas, SPEKE aplica las siguientes restricciones:
  - SPEKEno admite la verificación de firmas digitales (XMLDSIG) para las cargas útiles de solicitud o respuesta.
  - SPEKErequiere certificados RSA basados en 2048.
- Para flujos de trabajo clave rotativos, SPEKE requiere el `ContentKeyUsageRule` filtro,`KeyPeriodFilter`. SPEKEignora todos los demás `ContentKeyUsageRule` ajustes.
- SPEKE omite la funcionalidad `UpdateHistoryItemList`. Si la lista está presente en la respuesta, la SPEKE ignora.
- SPEKEadmite la rotación de teclas. SPEKEusa solo el `ContentKeyPeriod@index para rastrear el período clave.
- Para MSS PlayReady admitirlo, SPEKE usa un parámetro personalizado debajo de la `DRMSystem` etiqueta,`SPEKE:ProtectionHeader`.
- Para el HLS empaquetado, si `URIExtXKey` está presente en la respuesta, debe contener los datos completos para añadirlos al URI parámetro de la `EXT-X-KEY` etiqueta de una HLS lista de reproducción, sin necesidad de señalización adicional.
- En el caso de la lista de HLS reproducción, debajo de la `DRMSystem` SPEKE etiqueta, se muestran los parámetros personalizados opcionales `speke:KeyFormat` y`speke:KeyFormatVersions`, en el caso de las listas de reproducción, los valores `KEYFORMAT` y `KEYFORMATVERSIONS` los parámetros de la `EXT-X-KEY` etiqueta.

El vector de HLS inicialización (IV) siempre sigue al número de segmento, a menos que el operador lo especifique explícitamente.

- 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.
- SPEKEactualmente no admite varias pistas o claves por contenido.

  El SPEKE cifrador compatible actúa como cliente y envía `POST` las operaciones al punto final 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.

SPEKEAPIv1: componentes de carga útil estándar

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

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

```
<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 para el tipo de DRM sistema, registrado en la organización DASH IF. Para obtener 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 encabezad o contiene una referencia a los `kid` datos personalizados del proveedor`systemID`, además de datos personalizados del DRM proveedor, como parte de Common Encryption (CENC). El tipo de respuesta de clave debe ser esta o la respuesta `UriExtXKey` .

_Ejemplos de solicitudes de clave estándar y de PSSH _

El siguiente ejemplo muestra parte de un ejemplo de solicitud del cifrador al proveedor de DRM claves, con los componentes principales resaltados. La primera solicitud es para una clave estándar, mientras que la segunda es para obtener una PSSH respuesta:

```
<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>
```

_Ejemplos de respuestas para Standard Key y para PSSH _

El siguiente ejemplo muestra la respuesta correspondiente del proveedor de DRM claves al cifrador:

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

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

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

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

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

SPEKEAPIv1: ejemplos de llamadas a métodos de flujo de trabajo en vivo

Ejemplo de la sintaxis de la solicitud

El 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 CPIX elemento.

Encabezados de la solicitud

Nombre	Tipo	Se ejecuta	Descripción
`AWS Authorization`	Cadena	1..1	Consulte AWSSigv4

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

HTTP CODE	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	DASH- respuesta de CPIX carga útil
`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

El siguiente ejemplo muestra una carga útil típica de una solicitud en tiempo real desde el cifrador hasta el DRM proveedor de claves:

```
<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

El siguiente ejemplo muestra una carga útil de respuesta típica del proveedor de DRM claves:

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

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

```
  </cpix:DRMSystem>

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

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

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

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

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

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

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

SPEKEAPIv1: ejemplos de llamadas a métodos VOD de flujo de trabajo

Ejemplo de la sintaxis de la solicitud

El 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 CPIX elemento.

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

HTTP CODE	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	DASH- respuesta CPIX de carga útil
`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.

VODEjemplo de carga útil de solicitud con las claves en blanco

El siguiente ejemplo muestra una carga útil de VOD solicitud básica desde el cifrador hasta el DRM proveedor de claves:

```
<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>
```

VODEjemplo de carga útil de respuesta con las claves en blanco

El siguiente ejemplo muestra una carga útil de VOD respuesta básica del proveedor de DRM claves:

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

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

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

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

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

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

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

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

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

SPEKEAPIv1: cifrado de claves de contenido

Si lo desea, puede añadir el cifrado de claves de contenido a su SPEKE implementación. 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 AWS Cloud, los clientes importan los certificados al AWS Certificate Manager y, a continuación, utilizan el certificado resultante ARNs para sus actividades de cifrado. El cifrador usa el certificado ARNs y el ACM servicio para proporcionar claves de contenido cifradas al DRM proveedor de claves.

Restricciones

SPEKEadmite el cifrado de claves de contenido tal como se especifica en la CPIX especificación DASH -IF con las siguientes restricciones:

- SPEKEno admite la verificación de firma digital (XMLDSIG) para las cargas útiles de solicitud o respuesta.
- SPEKErequiere certificados RSA basados en 2048.

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

Implementación del cifrado de claves de contenido

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

- 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>
```

SPEKEAPIv1 - Latido

Ejemplo de la sintaxis de la solicitud

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

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

Respuesta de la solicitud

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

SPEKEAPIv1: anular el identificador clave

El cifrador crea un nuevo identificador de clave (KID) cada vez que rota las claves. Se lo pasa KID al proveedor de DRM claves en sus solicitudes. Casi siempre, el proveedor de claves responde de la misma maneraKID, pero puede proporcionar un valor diferente KID en la respuesta.

El siguiente es un ejemplo de solicitud con KID`11111111-1111-1111-1111-111111111111`:

```
   <cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke">
     <cpix:ContentKeyList>
      <cpix:ContentKey kid="11111111-1111-1111-1111-111111111111"></cpix:ContentKey>
     </cpix:ContentKeyList>
     <cpix:DRMSystemList>
      <!-- Common encryption (Widevine)-->
      <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
       <cpix:PSSH />
      </cpix:DRMSystem>
     </cpix:DRMSystemList>
     <cpix:ContentKeyPeriodList>
      <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
     </cpix:ContentKeyPeriodList>
     <cpix:ContentKeyUsageRuleList>
      <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111">
       <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
      </cpix:ContentKeyUsageRule>
     </cpix:ContentKeyUsageRuleList>
    </cpix:CPIX>
```

La siguiente respuesta anula el KID to`22222222-2222-2222-2222-222222222222`:

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

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

SPEKEAPIv2

Esta es la versión REST API 2 de Secure Packager and Encoder Key Exchange (SPEKE). Utilice esta especificación para proteger los DRM derechos de autor a los clientes que utilizan el cifrado. Para SPEKE cumplir con las normas, el proveedor de DRM claves debe exponer lo REST API descrito en esta especificación. El cifrador realiza API llamadas a su proveedor de claves.

> **Note**
>
> Los ejemplos de código de esta especificación se proporcionan únicamente con fines ilustrativos. No puede ejecutar los ejemplos porque no forman parte de una SPEKE implementación completa.

SPEKEutiliza la definición de estructura de datos del formato de intercambio de información sobre protección de contenido (DASH-IF-CPIX) del foro DASH industrial para el intercambio de claves, con algunas restricciones. DASH-IF- CPIX define un esquema para proporcionar un DRM intercambio múltiple y extensible desde la DRM plataforma 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 empaquetado de tasas de bits adaptables incluyenHLS, y. DASH MSS

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

SPEKEPor un lado, esto se aplica mediante el uso del `X-Speke-Version` HTTP encabezado y, por CPIX otro, mediante el uso del `CPIX@version` atributo. La falta de estos elementos en las solicitudes es típica de los flujos de trabajo heredados SPEKE de la versión 1. En los SPEKE flujos de trabajo de la versión 2, se espera que el proveedor de claves procese CPIX los documentos solo si admite ambos parámetros de versión.

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

En general, la SPEKE versión 2.0 presenta las siguientes evoluciones en comparación con la versión 1.0: SPEKE

- Todas las etiquetas del espacio de SPEKE XML nombres están en desuso en favor de etiquetas equivalentes en el espacio de nombres CPIX XML
- `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 obligatorios:, CPIX `CPIX@version` `ContentKey@commonEncryptionScheme`
- Nuevo CPIX elemento opcional: `DRMSystem.ContentProtectionData`
- Soporte para múltiples claves de contenido
- Mecanismo de control de versiones cruzado entre y SPEKE CPIX
- HTTPevolución de los encabezados: nuevo `X-Speke-Version` encabezado, `Speke-User-Agent` encabezado renombrado como `X-Speke-User-Agent`
- Depreciación de Heartbeat API

Como la especificación de la SPEKE versión 1.0 permanece inalterada, no es necesario que las implementaciones existentes cambien para seguir siendo compatibles SPEKE con los flujos de trabajo de la versión 1.0.

Temas

- SPEKEAPIv2: Personalizaciones y restricciones de la especificación -IF DASH
- SPEKEAPIv2: componentes de carga útil estándar

- SPEKEAPIv2 - Contrato de cifrado
- SPEKEAPIv2: ejemplos de llamadas a métodos de flujo de trabajo en vivo
- SPEKEAPIv2: ejemplos de llamadas a métodos VOD de flujo de trabajo
- SPEKEAPIv2: cifrado de claves de contenido
- SPEKEAPIv2: anular el identificador clave

SPEKEAPIv2: Personalizaciones y restricciones de la especificación -IF DASH

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

CPIXPerfil

- SPEKE sigue el flujo de trabajo Encriptador-Consumidor.
- En el caso de las claves de contenido cifradas, SPEKE se aplican las siguientes restricciones:
  - SPEKEno admite la verificación de firmas digitales (XMLDSIG) para las cargas útiles de solicitud o respuesta.
  - SPEKErequiere certificados RSA basados en 2048.
- SPEKEaprovecha solo un subconjunto de funcionalidades: CPIX
  - SPEKE omite la funcionalidad `UpdateHistoryItemList`. Si la lista está presente en la respuesta, la SPEKE ignora.
  - SPEKEOmite la funcionalidad de las teclas raíz/hoja. Si el `ContentKey@dependsOnKey` atributo está presente en la respuesta, SPEKE lo ignora.
  - SPEKEOmite el `BitrateFilter` elemento y el `VideoFilter@wcg` atributo. Si estos elementos o atributos están presentes en la CPIX carga útil, los SPEKE ignora.
- En los CPIX documentos intercambiados con la versión 2, 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. SPEKE
- Cuando el cifrador los incluya en una CPIX solicitud, todos los elementos y atributos deberán incluir un valor válido en la respuesta del proveedor CPIX de claves. De lo contrario, el encriptador se detendrá y generará un error.

- SPEKEadmite la rotación de claves con `KeyPeriodFilter` elementos. SPEKEutiliza únicamente el `ContentKeyPeriod@index` para realizar un seguimiento del período clave.
- Para la HLS señalización, se deben utilizar varios `DRMSystem.HLSSignalingData` elementos: uno con el valor de `DRMSystem.HLSSignalingData@playlist` atributo «media» y otro con el valor de `DRMSystem.HLSSignalingData@playlist` atributo «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 `CPIX@contentId`El proveedor de claves no puede anular un valor.

  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». Al recibir una solicitud con una versión no compatible, la descripción del error devuelta por el proveedor de claves será «CPIXUnsupported @version».

  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 «Falta ContentKey @ para». commonEncryptionScheme KID `id`

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

  No todos los `ContentKey@commonEncryptionScheme` valores son compatibles con todas las DRM tecnologías. Al recibir dicha combinación, 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`.

- Cuando reciba valores diferentes para `DRMSystem@PSSH` XML `<pssh>` un elemento `DRMSystem.ContentProtectionData` interno en el cuerpo de la CPIX respuesta, el cifrador se detendrá y arrojará un mensaje de error.

API para CPIX

- El proveedor de claves incluirá un valor para el encabezado de la `X-Speke-User-Agent` HTTP respuesta.
- Un SPEKE cifrador compatible actúa como cliente y envía POST las operaciones al punto final del proveedor de claves.
- El cifrador incluirá un valor para el encabezado de la `X-Speke-Version` HTTP solicitud y la SPEKE versión utilizada con la solicitud se formulará como. MajorVersion MinorVersion, como «2.0» para la SPEKE versión 2.0. Si el proveedor de claves no admite la SPEKE versión utilizada por el cifrador para la solicitud actual, devolverá un mensaje de error con la descripción «SPEKEVersión no compatible» y no intentará procesar el CPIX documento haciendo todo lo posible.

  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 cifrador mostrará un error y no volverá a intentar la solicitud con una versión de la versión 1.0. SPEKE

  Si el proveedor de claves no devuelve un error pero no devuelve un CPIX documento que incluya la información obligatoria, el cifrador 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 HTTP respuesta será un 4XX o un 5XX, nunca un 200. El código de error 422 se puede utilizar para todos los errores relacionados SPEKE con/. CPIX

Caso de error	Mensaje de error
CPIX@ no contentId está definido	Falta CPIX @ contentId
CPIX@version no está definido	Falta CPIX @version
CPIX@version no es compatible	@version no compatible CPIX

Caso de error	Mensaje de error
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 solo CPIX documento	commonEncryptionScheme Combinación ContentKey @ no compatible
ContentKey@ no commonEncryptionScheme es compatible con DRM la tecnología	ContentKey@ commonEncryptionScheme no es compatible con DRMSystem `id` (donde `id` es igual al systemId valor DRMSystem @)
El valor del encabezado de X-Speke-Version no es una versión compatible SPEKE	La versión del SPEKE no es compatible
El contrato de cifrado es incorrecto	Contrato de cifrado con formato incorrecto
El contrato de cifrado contradice DRM las restricciones de los niveles de seguridad	No se admite CPIX el contrato de cifrado solicitado
El contrato de cifrado no incluye VideoFilter ningún AudioFilter elemento	Falta el contrato CPIX de cifrado

SPEKEAPIv2: componentes de carga útil estándar

Mediante una sola SPEKE solicitud, el cifrador puede solicitar varias claves de contenido, junto con la señalización de manifiesto necesaria para varios formatos de empaquetado, de acuerdo con el contrato de cifrado definido para un contenido determinado.

Para cubrir todos estos aspectos, un CPIX documento 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.

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

Esta es una sección obligatoria, relevante tanto para la transmisión en directo como para la VOD transmisión, que define las diferentes claves de contenido que debe utilizar el cifrador.

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 CPIX especificación, los valores posibles del `ContentKey@commonEncryptionScheme` atributo se definen en la especificación sobre el cifrado común en los archivos con formato de archivo multimedia ISO básico (ISO/IEC23001-7:2016):

- 'cenc': AES - CTR modo de cifrado de muestras completas y submuestras de vídeo NAL
- 'cbc1': AES - CBC modo de cifrado de muestras completas y submuestras de vídeo NAL
- 'cens': AES - modo de cifrado parcial de patrones de vídeo CTR NAL
- 'cbcs': AES CBC modo de cifrado parcial del patrón de vídeo NAL

El siguiente ejemplo muestra un CPIX documento 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	contentId, versión, xmlns: cpix, xmlns: pskc	nombre, xmlns:enc	uno<cpix : >, uno<cpix : >, uno <cpix : >ContentKeyListDRMSystemListContentKeyUsageRuleList	uno<cpix : >, uno <cpix : >DeliveryDataListContentKeyPeriodList
<cpixContentKeyList: >	-	id	al menos un <cpix : >ContentKey	-
<cpix : >ContentKey	niño, Data commonEncryptionScheme	id, algoritmo, ExpliciTiv	un <pskc:Secret>	-
<pskc:Secret>	PlainValue o EncryptedValue	Valor MAC	-	<enc: EncryptionMethod >, <enc : >CipherData

sección <cpix : >DRMSystemList

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

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

```
<cpix:DRMSystemList>
 <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="9a04f079-9840-4286-ab92-e65be0885f95">
```

```
  <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master">HicXmbZ2m[...]jEi</cpix:HLSSignalingData>
  <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
  <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
 </cpix:DRMSystem>
</cpix:DRMSystemList>
```

Para obtener una lista completa DRMsystemIDs, 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 : >DRMSystemList	-	id	al menos un <cpix : >DRMSystem	-
<cpix : >DRMSystem	niño, systemId	niño, nombre, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHeaderData, dos elementos de <cpix: HLSSignalingData > con un valor de atributo de lista de reproducción diferente

`DRMSystem@PSSH`es obligatorio siISO: la BMFF encapsulación se aplica a los segmentos multimedia. `DRMSystem.ContentProtectionData`El cifrador aprovecha el XML `<pssh>` elemento interno solo con fines de señalización manifiesta.

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

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

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. UUIDsUsarlo 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 respaldado por 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 criptográficos, las claves de cifrado también deben adjuntarse a uno de los períodos criptográficos del CPIX documento, como se muestra en la sección siguiente.

sección <cpix : >ContentKeyUsageRuleList

Esta es una sección obligatoria, relevante tanto para la transmisión en directo como para la VOD transmisión, que define cómo las diferentes claves de contenido protegerán las pistas dentro de la retransmisión y durante los períodos criptográficos.

El elemento <cpix: ContentKeyUsageRuleList > puede contener uno o varios elementos secundarios de <cpix: ContentKeyUsageRule >. Cada uno de ellos describe las pistas a las que el cifrador aplica una clave de contenido determinada, posiblemente durante un periodo criptográfico 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 : >ContentKeyUsageRuleList	-	id	al menos un <cpix : >ContentKeyUsageRule	-
<cpix : >ContentKeyUsageRule	niño, intendedTrackType	-	al menos un <cpix: AudioFilter > o un <cpix : >(*) VideoFilter	<cpix : >KeyPeriodFilter
<cpix : >KeyPeriodFilter	periodId	-	-	-

Elemento compatible con SPEKE	Atributos obligatorios	Atributos opcionales	Elementos secundarios obligatorios	Elementos secundarios opcionales
<cpix : >AudioFilter	-	minChannels, maxChannels	-	-
<cpix : >VideoFilter	-	minPixels, hdrmaxPixels, 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._

SPEKEAPIv2 - 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 el cifrador debe indicarlo explícitamente en el CPIX documento que envíe el cifrador 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 `<cpix:ContentKeyUsageRuleList>` sección 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

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

CPIXtipo de filtro	SPEKESoporte general	Filtra los atributos compatibles con SPEKE	Los atributos de filtro no son compatibles con SPEKE
<cpix : >VideoFilter	Sí	minPixels, hdrmaxPixels,minFps, maxFps (atributos opcionales)	wcg
<cpix : >AudioFilter	Sí	minChannels, maxChannels (atributos opcionales)	
<cpix : >KeyPeriodFilter	Sí	periodId (atributo obligatorio)	
<cpix : >BitrateFilter	No	N/A	N/A
<cpix : >LabelFilter	No	N/A	N/A

Según la CPIX especificación 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 cifrador debe comprobar su configuración (externa a la CPIX carga útil) y comprobar que las pistas en cuestión no requieren cifrado. Si no	No es relevante: el proveedor de claves no conoce la estructura del streamset.

En esta situación	El encriptador debería/deberá...	El proveedor de claves debería/deberá...
	es lo esperado, el encriptador debería generar un error y detener el procesamiento.	
Varias reglas se superponen y sugieren múltiples claves de contenido para cifrar una pista específica	El cifrador debe aplicar las últimas que se hayan 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 SPEKE solicitud/respuesta	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 CPIX carga útil de la solicitud. SPEKE
Contrato de cifrado mal formado: intendedTrackType / Filters, excepción de restricción de cardinalidad, filtros o atributos no compatibles	El cifrador deberá establecer una excepción, detener el procesamiento y no enviar la SPEKE solicitud 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).

En esta situación	El encriptador debería/deberá...	El proveedor de claves debería/deberá...
Contrato de cifrado bien estructurado, pero que infringe las restricciones de los niveles de DRM seguridad: por ejemplo, se solicita una clave de contenido única para proteger tanto las pistas de audio como las pistas de vídeo UHD	Si el cifrador conoce las limitaciones de los niveles de DRM seguridad, debería hacer una excepción, detener el procesamiento y no enviar la SPEKE solicitud al proveedor de la clave, ya que lo más probable es que se traduzca en una protección del contenido errónea.	El proveedor de claves deberá establecer una excepción y devolverá el mensaje de error «No se admite el contrato de CPIX cifrado solicitado».
Contrato de cifrado faltante	El cifrador no enviará CPIX documentos que no contengan ningún elemento o elemento. VideoFilter AudioFilter	El proveedor de claves hará una excepción y devolverá el mensaje de error «Falta el contrato de CPIX cifrado».

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: varias 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///HD1HD2UHD1/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>
```

SPEKEAPIv2: ejemplos de llamadas a métodos de flujo de trabajo en vivo

Ejemplo de la sintaxis de la solicitud

El 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 CPIX documento.

Encabezados de la solicitud

Nombre	Tipo	Se ejecuta	Descripción
`AWS Authorization`	Cadena	1..1	Consulte AWSSigv4

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

Respuesta de la solicitud

HTTP CODE	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	DASH- respuesta de CPIX carga útil
`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

El siguiente ejemplo muestra una carga útil típica de solicitudes en directo desde el cifrador hasta el proveedor de claves, con una DRM 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

El siguiente ejemplo muestra una carga útil de respuesta típica del proveedor de DRM claves (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>
```

SPEKEAPIv2: ejemplos de llamadas a métodos VOD de flujo de trabajo

Ejemplo de la sintaxis de la solicitud

El 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 CPIX documento.

Encabezados de la solicitud

Nombre	Tipo	Se ejecuta	Descripción
`AWS Authorization`	Cadena	1..1	Consulte AWSSigv4
`X-Amz-Security-Token`	Cadena	1..1	Consulte Sigv4 AWS
`X-Amz-Date`	Cadena	1..1	Consulte Sigv4 AWS

Nombre	Tipo	Se ejecuta	Descripción
`Content-Type`	Cadena	1..1	application/xml
`X-Speke-Version`	Cadena	1..1	SPEKEAPIversión utilizada con la solicitud, formulada como MajorVersion. MinorVersion, como '2.0' para la SPEKE v2.0

Encabezados de la respuesta

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

Respuesta de la solicitud

HTTP CODE	Nombre de la carga	Se ejecuta	Descripción
`200 (Success)`	CPIX	1..1	DASH- respuesta de CPIX carga útil

HTTP CODE	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.

VODEjemplo de carga útil de solicitud con las claves en blanco

El siguiente ejemplo muestra una carga útil de VOD solicitud típica desde el cifrador hasta el proveedor de claves, con una DRM 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>
```

VODEjemplo de carga útil de respuesta con las claves en blanco

El siguiente ejemplo muestra una carga útil de respuesta típica del proveedor de DRM claves (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>
```

SPEKEAPIv2: cifrado de claves de contenido

Si lo desea, puede añadir el cifrado de claves de contenido a su SPEKE implementación. 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 AWS Cloud, los clientes importan los certificados al AWS Certificate Manager y, a continuación, utilizan el certificado resultante ARNs para sus actividades de cifrado. El cifrador usa el certificado ARNs y el ACM servicio para proporcionar claves de contenido cifradas al DRM proveedor de claves.

Restricciones

SPEKEadmite el cifrado de claves de contenido tal como se especifica en la CPIX especificación DASH -IF con las siguientes restricciones:

- SPEKEno admite la verificación de firma digital (XMLDSIG) para las cargas útiles de solicitud o respuesta.
- SPEKErequiere certificados RSA basados en 2048.

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

Implementación del cifrado de claves de contenido

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

- 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>
```

SPEKEAPIv2: anular el identificador clave

El cifrador crea un nuevo identificador de clave (KID) cada vez que rota las claves. Se lo pasa KID al proveedor de DRM claves en sus solicitudes. Casi siempre, el proveedor de claves responde de la misma maneraKID, pero puede proporcionar un valor diferente KID en la respuesta.

El siguiente es un ejemplo de solicitud con KID`11111111-1111-1111-1111-111111111111`:

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

```
   <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
  kid="11111111-1111-1111-1111-111111111111" commonEncryptionScheme="cbcs"></
 cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
   <!-- Widevine -->
   <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    <cpix:ContentProtectionData></cpix:ContentProtectionData>
    <cpix:PSSH></cpix:PSSH>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
   <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
  index="1" />
  </cpix:ContentKeyPeriodList>
  <cpix:ContentKeyUsageRuleList>
   <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111"
  intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
   </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
 </cpix:CPIX>
```

La siguiente respuesta anula el KID to`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 SPEKE API

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. Por medidas tecnológicas efectivas se entiende aquellas medidas que, en ausencia de la autoridad adecuada, no pueden eludirse en virtud de las leyes que cumplen las obligaciones establecidas en el artículo 11 del Tratado de Derecho de WIPO 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. Derechos morales, como el derecho de integridad, no están autorizados en virtud de la presente licencia pública, ni tampoco la publicidad, privacidad u otros derechos de personalidad similares; sin embargo, en la medida de lo posible, el licenciante renuncia y/o acuerda no hacer valer dichos derechos mantenidos por el licenciante de manera limitada a lo necesario para permitirle a usted ejercer los derechos con licencia, 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. indique que el Material Licenciado está licenciado bajo esta Licencia Pública e incluya el texto URI o el hiperenlace de esta Licencia Pública.

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 cumplir las condiciones proporcionando un recurso URI o un hipervínculo a un recurso que incluya la información requerida.
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 comparte material adaptado que produce, 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, el hipervínculo URI o el texto de la licencia de 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 para la guía de SPEKE socios y clientes

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

SPEKE v1

Cambio	Descripción	Fecha
Matriz de soporte: servicios y productos para AWS socios	Se agregó una nueva sección de SPEKE Support en los servicios y productos de los AWS socios, con una lista de los servicios de Bitmovin.	13 de enero de 2023
Actualizaciones de los proveedores de DRM plataformas	Se agregaron enlaces e información sobre nuevos socios a la lista de proveedor es de la DRM plataforma.	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 soporte - AWS Elemental Live	Se agregó una matriz de soporte de AWS Elemental Live.	27 de septiembre de 2018
Componentes de carga estándares	Se ha añadido una sección que define los elementos	27 de septiembre de 2018

Cambio	Descripción	Fecha
	principales de la JSON carga útil.	
KIDanular	Se agregó una sección sobre las KID anulaciones por parte de un proveedor de claves.	27 de septiembre de 2018
Se corrigieron los enlaces al sitio DASH -IF	Se corrigieron los enlaces al sitio DASH IF para la CPIX especificación y para la IDs página del sistema.	27 de septiembre de 2018
Copia de publicación para AWS Elemental Live	Se actualizó la SPEKE documentación para incluir los productos de AWS Elemental.	20 de julio de 2018
CMAF	Se actualizaron las tablas matriciales de soporte de los servicios para incluir el formato de aplicación multimedia común (CMAF).	27 de junio de 2018
Versión inicial	Versión inicial de la versión 1 de Secure Packager and Encoder Key Exchange (SPEKE), una especificación para la comunicación entre un cifrador de contenido y un DRM proveedor de claves. El proveedor de DRM claves ofrece un intercambio de claves Secure Packager y Encoder para gestionar las solicitudes de claves entrantes . API	27 de noviembre de 2017

SPEKE v2

Cambio	Descripción	Fecha
Actualizaciones de la sección de proveedores de DRM plataformas y de la sección de soporte AWS de servicios y productos SPEKE	Se agregó Webstream a la columna SPEKE v2 de la lista de proveedores de DRM plataformas y MediaConvert a la columna SPEKE v2 de la tabla de SPEKE soporte en AWS servicios y productos.	10 de octubre de 2024
Actualizaciones de la sección DRM de proveedores de plataformas	Se han añadido nuevos socios cualificados a la columna SPEKE v2 de la lista de proveedores de DRM plataformas.	9 de agosto de 2023
Actualizaciones de las secciones de ejemplos de llamadas a métodos en vivo y de VOD flujo de trabajo	Se agregó el encabezado de X-Speke-Version respuesta que faltaba en las secciones de ejemplos de llamadas a métodos VOD de flujo de trabajo y Live de la SPEKE versión 2.	13 de enero de 2023
Actualizaciones de los proveedores de DRM plataformas y de la sección de contratos de cifrado	Se han añadido nuevos socios cualificados a la columna SPEKE v2 de la lista de proveedores de DRM plataformas. Se han añadido dos nuevos ejemplos de contratos de cifrado y se ha cambiado la resolució n máxima de SD a 1024 x 576 en todos los ejemplos correspondientes.	27 de enero de 2022

Cambio	Descripción	Fecha
Lanzamiento inicial	Versión inicial de la versión 2.0 de Secure Packager and Encoder Key Exchange (SPEKE), una especificación para la comunicación entre un cifrador de contenido y un DRM proveedor de claves. El proveedor de DRM claves ofrece un intercambio de claves Secure Packager y Encoder para gestionar las solicitudes de claves entrantes . API	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.