Guia de parceiros e clientes

Especificação da API do Secure Packager and Encoder Key Exchange

Especificação da API do Secure Packager and Encoder Key Exchange: Guia de parceiros e clientes

Table of Contents

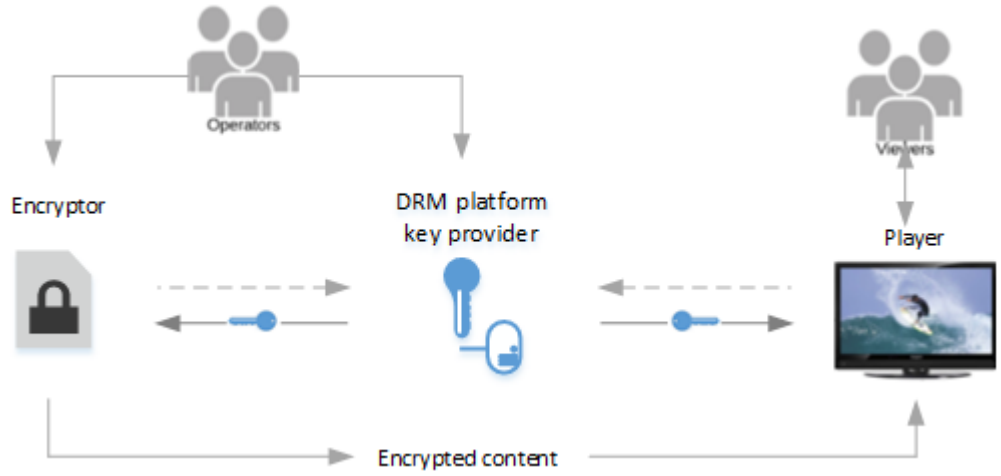
O que é o Secure Packager and Encoder Key Exchange?

O Secure Packager and Encoder Key Exchange (SPEKE) define o padrão de comunicação entre os criptografadores e os empacotadores de provedores de chaves de conteúdo de mídia e de gerenciamento de direitos digitais (DRM). A especificação trata dos criptografadores em execução on-premises e na Nuvem AWS.

Tópicos

Arquitetura geral

A ilustração a seguir mostra uma visão detalhada da arquitetura de criptografia de conteúdo do SPEKE para produtos on-premises.



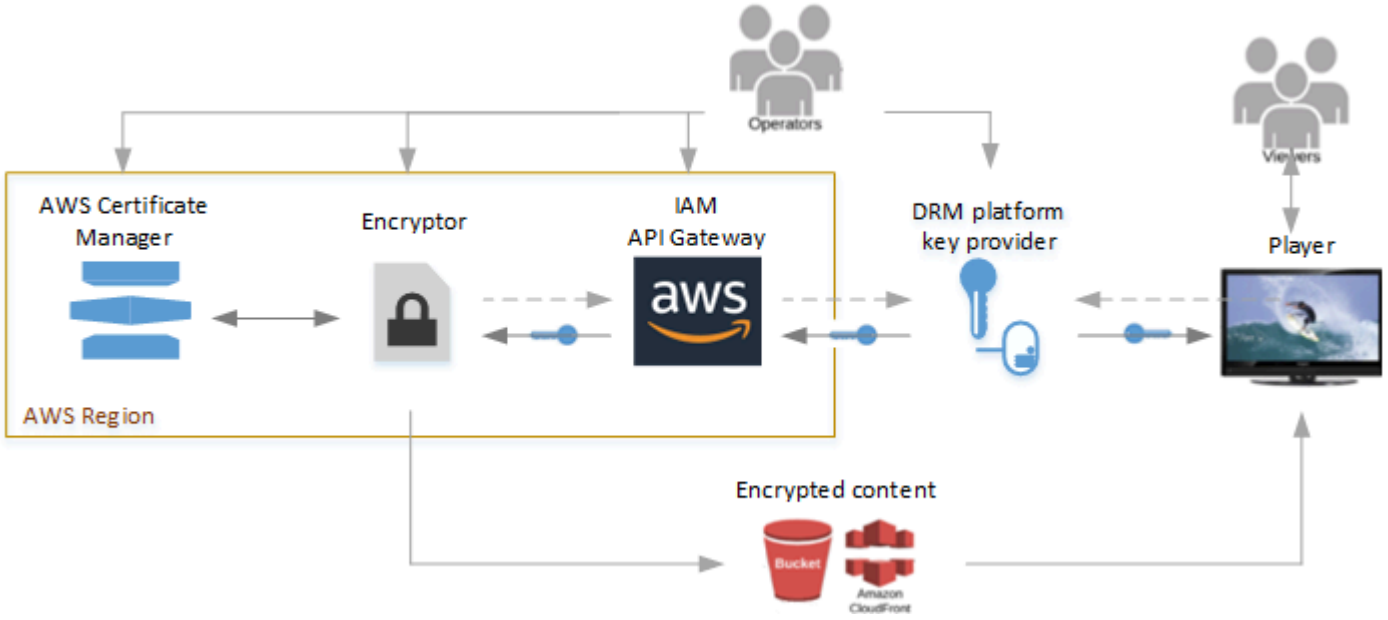
Esses são os principais componentes da arquitetura anterior:

- Criptografador: fornece a tecnologia de criptografia. Recebe as solicitações de criptografia do operador e recupera as chaves necessárias do servidor de chaves de DRM para proteger o conteúdo criptografado.
- Provedor de chaves de plataforma de DRM: fornece chaves de criptografia para o criptografador por meio de uma API em conformidade com o SPEKE. O provedor também fornece licenças de criptografia para os media players.

- Player: solicita chaves do mesmo provedor de chaves de plataforma de DRM, as quais o player usa para desbloquear o conteúdo e enviar aos visualizadores.

Arquitetura baseada na Nuvem AWS

A ilustração a seguir mostra a arquitetura de alto nível quando o SPEKE é usado com os serviços e recursos executados na Nuvem AWS.



Estes são os principais serviços e componentes:

- Criptografador: fornece a tecnologia de criptografia na Nuvem AWS. O criptografador recebe as solicitações de criptografia do operador e recupera as chaves necessárias do provedor de chaves de DRM, por meio do Amazon API Gateway, para proteger o conteúdo criptografado. Ele entrega o conteúdo criptografado em um bucket do Amazon S3 ou por meio de uma distribuição da Amazon CloudFront .
- AWS IAM e Amazon API Gateway: gerenciam funções confiáveis do cliente e a comunicação proxy entre o criptografador e o provedor de chaves. O API Gateway fornece recursos de registro em log e permite que os clientes controlem as relações com o criptografador e a plataforma de DRM. Os clientes permitem o acesso do provedor de chaves configurando a função do IAM. O API Gateway deve residir na mesma região da AWS que o criptografador.
- AWS Certificate Manager (Opcional): fornece o gerenciamento de certificados para criptografia de chaves de conteúdo. A criptografia de chaves de conteúdo é a prática recomendada para uma

comunicação segura. O gerenciador de certificados deve residir na mesma região da AWS que o criptografador.

- Provedor de chaves de plataforma de DRM: fornece chaves de criptografia para o criptografador por meio de uma API em conformidade com o SPEKE. O provedor também fornece licenças de criptografia para os media players.
- Player: solicita chaves do mesmo provedor de chaves de plataforma de DRM, as quais o player usa para desbloquear o conteúdo e enviar aos visualizadores.

Como começar a usar

Para obter um material introdutório adicional sobre o SPEKE, consulte Você é iniciante no SPEKE?.

Você é cliente?

Faça uma parceria com um provedor de plataforma de DRM do AWS Elemental para configurar e usar a criptografia. Para obter detalhes, consulte Integração do cliente.

Você é um provedor de plataforma de DRM ou um cliente com seu próprio provedor de chaves?

Exponha uma API REST para seu provedor de chaves em conformidade com a especificação do SPEKE. Para obter detalhes, consulte a especificação da API SPEKE.

Você é iniciante com o SPEKE?

Esta seção fornece um material introdutório para leitores iniciantes no Secure Packager and Encoder Key Exchange (SPEKE).

Para uma introdução ao SPEKE, assista ao seguinte webcast:

Especificações e serviços relacionados

- Permissões da API Gateway: como controlar o acesso a uma API com permissões do AWS Identity and Access Management (AWS IAM).
- AWS AssumeRole — Como usar o AWS Security Token Service (AWS STS) para assumir a funcionalidade da função.
- AWS Sigv4: como assinar uma solicitação HTTP usando o Signature versão 4.
- Especificação CPIX do DASH-IF v2.0: a especificação de Content Protection Information Exchange Format (CPIX), na qual se baseia essa especificação do SPEKE v.1.0.
- Especificação CPIX do DASH-IF v2.3: a especificação de Content Protection Information Exchange Format (CPIX), na qual se baseia essa especificação do SPEKE v.2.0.
- IDs do sistema DASH-IF: a lista de identificadores registrados para os sistemas de DRM.
- https://github.com/awslabs/ speke-reference-server — Exemplo de provedor de chave de referência para usar com sua conta da AWS, para ajudar você a começar com uma implementação do SPEKE na AWS.

Terminologia

A lista a seguir define a terminologia usada na especificação. Sempre que possível, essa especificação segue a terminologia usada na especificação do CPIX DASH-IF.

- ARN: nome de recurso da Amazon. Identifica exclusivamente um recurso da AWS.
- Chave de conteúdo: uma chave criptográfica usada para criptografar parte do conteúdo.
- Provedor de conteúdo: um fornecedor que oferece os direitos e as regras para a entrega de mídias protegidas. O provedor de conteúdo também pode fornecer mídias de origem (formato mezzanine, para transcodificação), identificadores de ativos, identificadores de chave (KIDs), valores de chave, instruções de codificação e metadados de descrição de conteúdo.

- DRM: gerenciamento de direitos digitais. Usado para assegurar conteúdo digital protegido por direitos autorais contra acesso não aprovado.
- Plataforma de DRM: um sistema que fornece funcionalidade de DRM e suporte a criptografadores e visualizadores de conteúdo, incluindo o fornecimento de chaves de DRM e o licenciamento para criptografar e descriptografar conteúdo.
- Provedor de DRM: consulte "Plataforma de DRM".
- Sistema de DRM: um padrão para implementações de DRM. Os sistemas DRM comuns incluem Apple FairPlay, Google Widevine e Microsoft. PlayReady Os sistemas de DRM são usados pelos provedores de conteúdo para assegurar o conteúdo digital a ser entregue para os visualizadores e o acesso a ele. Para obter uma lista de sistemas de DRM registrados com o DASH-IF, consulte IDs do sistema DASH-IF. A especificação CPIX DASH-IF usa o termo "sistema de DRM" conforme definido aqui e, em alguns lugares, usa "sistema de DRM" para significar o que a especificação chama de plataforma de DRM.
- Solução de DRM: consulte "Plataforma de DRM".
- Tecnologia de DRM: consulte "Sistema de DRM".
- Criptografador: um componente de processamento de mídia que criptografa o conteúdo de mídia usando chaves obtidas do provedor de chaves. Normalmente, os criptografadores também adicionam sinalização de criptografia de DRM e metadados à mídia. Os criptografadores geralmente são codificadores, empacotadores e transcodificadores.
- Provedor de chaves: o componente de uma plataforma de DRM que expõe uma API REST do SPEKE para lidar com as solicitações de chaves. O provedor de chaves pode ser o próprio servidor de chaves ou outro componente da plataforma.
- Servidor de chaves: o componente de uma plataforma de DRM que mantém as chaves de criptografia e descriptografia de conteúdo.
- Operador: pessoa responsável pela operação de todo o sistema operacional, incluindo o criptografador e provedor de chaves.
- Player: um media player em operação em nome de um visualizador. Obtém suas informações de diferentes fontes, incluindo os arquivos manifesto de mídias, arquivos de mídia e licenças de DRM. Solicita as licenças no servidor de DRM em nome dos visualizadores.

Integração de clientes

Proteja seu conteúdo contra o uso não autorizado combinando um servidor de chaves sistema de gerenciamento de direitos digitais (DRM), Secure Packager and Encoder Key Exchange (SPEKE), com seu criptografador de conteúdo de mídia e seus media players. O SPEKE define o padrão de comunicação entre os criptografadores e os empacotadores de provedores de chaves de conteúdo de mídia e de gerenciamento de direitos digitais (DRM). Para integrar, escolha um provedor de chaves de plataforma de DRM e configure a comunicação entre o provedor de chaves e seus criptografadores e players.

Tópicos

Integrar um provedor de plataforma de DRM

Os seguintes parceiros da Amazon fornecem implementações da plataforma de DRM para SPEKE. Para obter detalhes das soluções e informações sobre como contatá-los, siga os links para as páginas deles na rede de parceiros da Amazon. Parceiros que não têm um link não possuem uma página do Amazon Partner Network atualmente, mas você pode entrar em contato com eles diretamente. Os parceiros podem ajudar você a se preparar para usar as plataformas.

Provedor de plataforma de DRM	Suporte para SPEKE v1	Suporte ao SPEKE v2 (AWS Elemental) MediaPackage
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKA Entworks	√	√

Provedor de plataforma de DRM	Suporte para SPEKE v1	Suporte ao SPEKE v2 (AWS Elemental) MediaPackage
Insys Cloud DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√
JW Player	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	

Suporte do SPEKE em serviços e produtos da AWS

Esta seção lista o suporte ao SPEKE fornecido pelos AWS Media Services executados na Nuvem AWS e pelos produtos de mídia on-premises da AWS. Esses serviços e produtos são os criptografadores na arquitetura de criptografia de conteúdo SPEKE. Verifique se o protocolo de streaming e o sistema de DRM que você deseja estão disponíveis para o produto ou serviço.

Serviço ou produto da AWS	Suporte para SPEKE v1	Suporte para SPEKE v2	Tecnologias de DRM compatíveis
AWS Elemental MediaConvert — serviço executado na nuvem da AWS	√		Documentação

Serviço ou produto da AWS	Suporte para SPEKE v1	Suporte para SPEKE v2	Tecnologias de DRM compatíveis
AWS Elemental MediaPackage — serviço executado na nuvem da AWS	√	√	Documentação
AWS Elemental Live: Produto on-premises	√		Documentação: MPEG-DASH / HLS
Servidor AWS Elemental: Produto on-premises	√		Documentação

Suporte do SPEKE em serviços e produtos de parceiro da AWS

Esta seção lista o suporte ao SPEKE fornecido pelos serviços e produtos de parceiro da AWS executados na Nuvem AWS. Esses serviços e produtos são os criptografadores na arquitetura de criptografia de conteúdo SPEKE. Verifique se o protocolo de streaming e o sistema de DRM que você deseja estão disponíveis para o produto ou serviço.

Serviço ou produto da AWS	Suporte para SPEKE v1	Suporte para SPEKE v2	Tecnologias de DRM compatíveis
Codificação de vídeo ao vivo Bitmovin	√		Documentação
Codificação de vídeo sob demanda (VOD) Bitmovin	√		Documentação

Especificação da API SPEKE

Essa é a especificação da API REST para o Secure Packager and Encoder Key Exchange (SPEKE). Use esta especificação para fornecer a proteção de direitos autorais de DRM aos clientes que usam criptografia.

Em um fluxo de trabalho de streaming de vídeo, o mecanismo de criptografia se comunica com o provedor de chaves de plataforma de DRM para solicitar as chaves de conteúdo. Essas chaves são altamente confidenciais. Portanto, é fundamental que o provedor de chaves e o mecanismo de criptografia estabeleçam um canal de comunicação altamente seguro e confiável. Você também pode criptografar as chaves de conteúdo no documento para obter uma end-to-end criptografia mais segura.

Essa especificação aborda os seguintes objetivos:

- Defina uma interface simples, confiável e altamente segura que os clientes e os fornecedores de DRM possam usar para integrar com os criptografadores quando a criptografia de conteúdo for necessária.
- Abranja os fluxos de trabalho em tempo real e de VOD e inclua as condições de erro e os mecanismos de autenticação necessários para uma comunicação forte e altamente segura entre os criptografadores e os endpoints do provedor de chaves de DRM.
- Inclua suporte para embalagens HLS, MSS e DASH e seus sistemas DRM comuns:, FairPlay, PlayReady e Widevine/CENC.
- Manter a especificação simples e extensível, para oferecer suporte a futuros sistemas DRM.
- Usar uma API REST simples.

> **Note**
>
>

SER RESPONSABILIZADOS POR QUALQUER RECLAMAÇÃO, DANO OU OUTRA OBRIGAÇÃO, SEJA EM CASO DE AÇÃO CONTRATUAL OU OUTRO ATO ILÍCITO PROVENIENTE DE OU ASSOCIADO A ESTE MATERIAL, SEU USO OU A OUTROS PROCEDIMENTOS NO MATERIAL.

Tópicos

Autenticação

O SPEKE requer autenticação para produtos on-premises e para serviços e recursos executados na Nuvem AWS.

Tópicos

Autenticação para implementações na Nuvem AWS

O SPEKE requer a autenticação da AWS por meio de funções do IAM para uso com um criptografador. As funções do IAM são criadas pelo provedor de DRM ou pelo operador proprietário do endpoint de DRM em uma conta da AWS. Cada função é atribuída um nome de recurso da Amazon (ARN), que o operador de serviço do AWS Elemental fornece no console do serviço ao solicitar a criptografia. As permissões de política da função devem estar configuradas para dar permissão de acesso à API do provedor de chaves e nenhum outro acesso a recursos da AWS. Quando o criptografador entra em contato com o provedor de chaves de DRM, ele usa o ARN da função para assumir a função do provedor de chaves da conta, que retorna credenciais temporárias para o criptografador usar e acessar o provedor de chaves.

Uma implementação comum é para o operador ou a plataforma de DRM usar o Amazon API Gateway na frente do provedor de chaves e, então, habilitar a autorização do AWS Identity and

Access Management (AWS IAM) no recurso do API Gateway. Você pode usar o seguinte exemplo de definição de política e anexá-lo a uma nova função para conceder as permissões adequadas ao recurso. Neste caso, as permissões são para todos os recursos do API Gateway.

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

Por fim, a função requer a adição de uma relação de confiança, e o operador deve ser capaz de selecionar o serviço.

O exemplo a seguir mostra um ARN de função criado para acessar o provedor de chaves de DRM:

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

Para obter mais informações sobre a criação de uma função, consulte AWS AssumeRole. Para obter mais informações sobre a assinatura de uma solicitação, consulte AWS Sigv4.

Autenticação para produtos on-premises

Para produtos on-premises, recomendamos usar autenticação SSL/TLS e Digest para obter a melhor segurança, mas, no mínimo, você deve usar a autenticação básica por HTTPS.

Os dois tipos de autenticação usam o cabeçalho `Authorization` na solicitação HTTP:

- Autenticação Digest – O cabeçalho de autorização consiste no identificador `Digest` seguido por uma série de valores que autenticam a solicitação. Especificamente, um valor de resposta é gerado por meio de uma série de funções de hash MD5 que incluem um one-time-use nonce exclusivo do servidor que é usado para garantir que a senha seja transmitida com segurança.

- Autenticação Basic – O cabeçalho de autorização consiste no identificador `Basic` seguido por uma string codificada no formato base-64 que representa o nome de usuário e a senha, separados por dois-pontos.

Para obter informações sobre a autenticação Basic e Digest, incluindo informações detalhadas sobre o cabeçalho, consulte a especificação de Internet Engineering Task Force (IETF) RFC 2617 - Autenticação HTTP: Autenticação de acesso Basic e Digest.

API SPEKE v1

Para estar em conformidade com o SPEKE, seu provedor de chaves de DRM deve expor a API REST descrita nesta especificação. O criptografador faz chamadas de API ao seu provedor de chaves.

> **Note**
>
> Os exemplos de código nesta especificação são apenas para fins de ilustração. Você não pode executar os exemplos porque eles não fazem parte de uma implementação completa do SPEKE.

O Secure Packager and Encoder Key Exchange usa a definição de estrutura de dados DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) para troca de chaves, com algumas restrições. O CPIX do DASH-IF define um esquema para fornecer uma troca extensível e multi-DRM da plataforma de DRM ao criptografador. Isso permite a criptografia de conteúdo para todos os formatos adaptáveis de empacotamento de taxa de bits no momento da compactação de conteúdo e empacotamento. Os formatos adaptáveis de empacotamento de taxa de bits incluem HLS, DASH e MSS.

Para obter informações detalhadas sobre o formato de troca, consulte a especificação CPIX do DASH Industry Forum em https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf.

Tópicos

- API SPEKE v1: Exemplos de chamadas de método de fluxo de trabalho de VOD
- API SPEKE v1: Criptografia de chave de conteúdo
- API SPEKE v1: Heartbeat
- SPEKE API v1: Substituindo o identificador de chave

API SPEKE v1: Personalizações e restrições para a especificação do DASH-IF

A especificação CPIX do DASH-IF https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf suporta vários casos de uso e topologias. A especificação da API SPEKE adere à especificação CPIX com as seguintes personalizações e restrições:

- O SPEKE segue o fluxo de trabalho de criptografador e consumidor.
- Para chaves de conteúdo criptografadas, o SPEKE aplica as seguintes restrições:
  - O SPEKE não oferece suporte à verificação de assinatura digital (XMLDSIG) para cargas de solicitação ou resposta.
  - O SPEKE exige 2048 certificados baseados em RSA.
- Para fluxos de trabalho de chaves rotativas, o SPEKE requer o `ContentKeyUsageRule` filtro, `KeyPeriodFilter`. O SPEKE ignora todas as outras `ContentKeyUsageRule` configurações.
- O SPEKE omite a funcionalidade `UpdateHistoryItemList`. Se a lista estiver presente na resposta, o SPEKE vai ignorá-la.
- O SPEKE suporta alternância de chaves. O SPEKE usa somente o `ContentKeyPeriod@index para rastrear o período chave.
- Para oferecer suporte ao MSS PlayReady, o SPEKE usa um parâmetro personalizado sob a `DRMSystem` tag,. `SPEKE:ProtectionHeader`
- Para o empacotamento HLS, se `URIExtXKey` estiver presente na resposta, ele deve conter os dados completos para adicionar no parâmetro de URI da tag `EXT-X-KEY` de uma lista de reprodução HLS, com nenhum outro requisito de sinalização.
- Para a lista de reprodução HLS na tag `DRMSystem`, o SPEKE fornece os parâmetros personalizados opcionais `speke:KeyFormat` e `speke:KeyFormatVersions` para os valores dos parâmetros `KEYFORMAT` e `KEYFORMATVERSIONS` da tag `EXT-X-KEY`.

  O vetor de inicialização (IV) HLS sempre segue número do segmento, a menos que especificado explicitamente pelo operador.

- Ao solicitar chaves, o criptografador pode usar o atributo opcional `@explicitIV` no elemento `ContentKey`. O provedor de chaves pode responder com um IV usando `@explicitIV`, mesmo se o atributo não estiver incluído na solicitação.
- O criptografador cria o identificador de chaves (`KID`), que permanece o mesmo para qualquer período de chave e ID de conteúdo. O provedor de chaves inclui o servidor `KID` na resposta ao documento da solicitação.
- O provedor de chaves pode incluir um valor para o cabeçalho da resposta `Speke-User-Agent`, para se identificar para fins de depuração.
- O SPEKE não oferece suporte a vários controles ou chaves por conteúdo.

  O criptografador em conformidade com o SPEKE atua como um cliente e envia operações `POST` ao endpoint do provedor de chaves. O criptografador pode enviar uma solicitação `heartbeat` periódica para garantir a integridade da conexão entre o criptografador e o endpoint do provedor de chaves.

API SPEKE v1: Componentes de carga útil padrão

Em qualquer solicitação do SPEKE, o criptografador pode solicitar respostas para um ou mais sistemas de DRM. O criptografador especifica os sistemas de DRM no `<cpix:DRMSystemList>` da carga da solicitação. Cada especificação do sistema inclui a chave e indica o tipo de resposta a ser retornada.

O exemplo a seguir mostra uma lista de sistemas DRM com uma única especificação do sistema DRM:

```
<cpix:DRMSystemList>
    <!--HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    systemId="81376844-f976-481e-a84e-cc25d39b0b33">
        <cpix:URIExtXKey></cpix:URIExtXKey>
        <speke:KeyFormat></speke:KeyFormat>
        <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>
</cpix:DRMSystemList>
```

A tabela a seguir lista os principais componentes de cada `<cpix:DRMSystem>`.

Identificador	Description
`systemId` ou `schemeId`	Identificador exclusivo para o tipo de sistema DRM, conforme registrado na organização do DASH IF. Para obter uma lista, consulte IDs do sistema DASH-IF.
`kid`	O ID da chave. Essa não é a chave real, mas sim um identificador que aponta para a chave em uma tabela de hash.
`<cpix:UriExtXKey>`	Solicita uma chave padrão não criptografada. O tipo de resposta da chave deve ser este, ou a resposta `PSSH`.
`<cpix:PSSH>`	Solicita um Protection System Specific Header (PSSH). Esse tipo de cabeçalho contém uma referência a `kid`, `systemID`, além de dados personalizados para o fornecedor de DRM, como parte do Common Encryption (CENC). O tipo de resposta da chave deve ser este, ou a resposta `UriExtXKey` .

Solicitações de exemplo para chave padrão e para PSSH _

O exemplo a seguir mostra parte de uma amostra de solicitação do criptografador para o provedor de chaves de DRM, com os principais componentes destacados. A primeira solicitação é para uma chave padrão, enquanto a segunda solicitação é para uma resposta PSSH:

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

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

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

_ Respostas de exemplo para chave padrão e para PSSH _

A lista a seguir mostra a resposta correspondente do provedor de chaves de DRM para o criptografador:

```
<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>
```

API SPEKE v1: Exemplos de chamadas de método de fluxo de trabalho em tempo real

Exemplo de sintaxe de solicitação

O seguinte URL é um exemplo e não indica um formato fixo:

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

Corpo da solicitação

Um elemento CPIX.

Cabeçalhos de solicitação

Nome	Tipo	Ocorre	Descrição
`AWS Authorization`	Cadeia de caracteres	1..1	Consulte AWS Sigv4
`X-Amz-Security-Token`	String	1..1	Consulte AWS Sigv4
`X-Amz-Date`	String	1..1	Consulte AWS Sigv4
`Content-Type`	String	1..1	application/xml

Cabeçalhos de resposta

Nome	Tipo	Ocorre	Descrição
`Speke-User-Agent`	Cadeia de caracteres	1..1	String que identifica o provedor de chaves
`Content-Type`	String	1..1	application/xml

Resposta de solicitação

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`200 (Success)`	CPIX	1..1	Resposta da carga DASH-CPIX:
`4XX (Client error)`	Mensagem de erro do cliente	1..1	Descrição do erro do cliente
`5XX (Server error)`	Mensagem de erro do servidor	1..1	Descrição de erro do servidor

> **Note**
>
> Os exemplos nesta seção não incluem a criptografia de chaves de conteúdo. Para obter informações sobre como adicionar criptografia de chaves de conteúdo, consulte Criptografia de chaves de conteúdo.

Exemplo de carga de solicitação em tempo real com chaves em branco

O exemplo a seguir mostra uma carga típica de solicitação em tempo real do criptografador para o provedor de chaves DRM:

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

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

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

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

Exemplo de carga de resposta em tempo real com chaves em branco

O exemplo a seguir mostra uma carga típica de resposta em tempo real do provedor de chaves de DRM:

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

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

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

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

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

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

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

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

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

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

API SPEKE v1: Exemplos de chamadas de método de fluxo de trabalho de VOD

Exemplo de sintaxe de solicitação

O seguinte URL é um exemplo e não indica um formato fixo.

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

Corpo da solicitação

Um elemento CPIX.

Cabeçalhos de resposta

Nome	Tipo	Ocorre	Descrição
`Speke-User-Agent`	Cadeia de caracteres	1..1	String que identifica o provedor de chaves
`Content-Type`	String	1..1	application/xml

Resposta de solicitação

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`200 (Success)`	CPIX	1..1	Resposta da carga DASH-CPIX:
`4XX (Client error)`	Mensagem de erro do cliente	1..1	Descrição do erro do cliente

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`5XX (Server error)`	Mensagem de erro do servidor	1..1	Descrição de erro do servidor

> **Note**
>
> Os exemplos nesta seção não incluem a criptografia de chaves de conteúdo. Para obter informações sobre como adicionar criptografia de chaves de conteúdo, consulte Criptografia de chaves de conteúdo.

Exemplo de carga de solicitação de VOD com chaves em branco

O exemplo a seguir mostra uma carga de solicitação de VOD básica do criptografador para o provedor de chaves de DRM:

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

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

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

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

Exemplo de carga de resposta de VOD com chaves em branco

O exemplo a seguir mostra uma carga básica de resposta de VOD do provedor de chaves DRM:

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

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

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

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

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

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

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

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

API SPEKE v1: Criptografia de chave de conteúdo

Também é possível adicionar a criptografia de chaves de conteúdo à sua implementação do SPEKE. A criptografia da chave de conteúdo garante end-to-end proteção total ao criptografar as chaves de conteúdo para trânsito, além de criptografar o próprio conteúdo. Se não a implementar no

seu provedor de chaves, dependerá apenas da criptografia de camada de transporte e da forte autenticação para segurança.

Para usar a criptografia de chaves de conteúdo em criptografadores executados na Nuvem AWS, clientes importam certificados para o AWS Certificate Manager e, depois, usam os ARNs do certificado resultante nas atividades de criptografia. O criptografador usa os ARNs dos certificados e o serviço do ACM para fornecer chaves de conteúdo criptografadas para o provedor de chaves de DRM.

Restrições

O SPEKE oferece suporte à criptografia de chaves de conteúdo, conforme detalhado na especificação CPIX do DASH-IF, com as seguintes restrições:

- O SPEKE não oferece suporte à verificação de assinatura digital (XMLDSIG) para cargas de solicitação ou resposta.
- O SPEKE exige 2048 certificados baseados em RSA.

Essas restrições também estão listadas em Personalizações e restrições à especificação DASH-IF.

Implementar a criptografia de chaves de conteúdo

Para oferecer a criptografia de chaves de conteúdo, inclua o seguinte em suas implementações do provedor de chaves DRM:

- Gerencie o elemento `<cpix:DeliveryDataList>` nas cargas de solicitação e de resposta.
- Forneça valores criptografados em `<cpix:ContentKeyList>` das cargas de resposta.

Para obter mais informações sobre esses elementos, consulte a Especificação do DASH-IF CPIX 2.0.

Exemplo de elemento de criptografia de chaves de conteúdo `<cpix:DeliveryDataList>` na carga de solicitação

O exemplo a seguir destaca em negrito o elemento `<cpix:DeliveryDataList>` adicionado:

```
<?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>
```

Exemplo de elemento de criptografia de chaves de conteúdo `<cpix:DeliveryDataList>` na carga de resposta

O exemplo a seguir destaca em negrito o elemento `<cpix:DeliveryDataList>` adicionado:

```
<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>
```

Exemplo de elemento de criptografia de chaves de conteúdo `<cpix:ContentKeyList>` na carga de resposta

O exemplo a seguir mostra o tratamento das chaves de conteúdo criptografadas no elemento `<cpix:ContentKeyList>` da carga de resposta. O elemento `<pskc:EncryptedValue>` é usado:

```
   <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>
```

Por comparação, o exemplo a seguir mostra uma carga de resposta semelhante à chave de conteúdo entregue sem criptografia, como uma chave em branco. O elemento `<pskc:PlainValue>` é usado:

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

API SPEKE v1: Heartbeat

Exemplo de sintaxe de solicitação

O seguinte URL é um exemplo e não indica um formato fixo:

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

Resposta de solicitação

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`200 (Success)`	statusMessage	1..1	Mensagem que descreve o status

SPEKE API v1: Substituindo o identificador de chave

O criptografador cria um novo identificador de chave (KID) sempre que ele alterna chaves. Ele repassa o KID para o provedor de chaves de DRM nas solicitações. Quase sempre, o provedor de chaves responde usando o mesmo KID, mas pode fornecer um valor diferente para o KID na resposta.

O seguinte é uma solicitação de exemplo com o 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>
```

A seguinte resposta substitui o KID por `22222222-2222-2222-2222-222222222222`:

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

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

API SPEKE v2

Para estar em conformidade com o SPEKE, seu provedor de chaves de DRM deve expor a API REST descrita nesta especificação. O criptografador faz chamadas de API ao seu provedor de chaves.

> **Note**
>
> Os exemplos de código nesta especificação são apenas para fins de ilustração. Você não pode executar os exemplos porque eles não fazem parte de uma implementação completa do SPEKE.

O Secure Packager and Encoder Key Exchange usa a definição de estrutura de dados DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) para troca de chaves, com algumas restrições. O CPIX do DASH-IF define um esquema para fornecer uma troca extensível e multi-DRM da plataforma de DRM ao criptografador. Isso permite a criptografia de conteúdo para todos os formatos adaptáveis de empacotamento de taxa de bits no momento da compactação de conteúdo e empacotamento. Os formatos adaptáveis de empacotamento de taxa de bits incluem HLS, DASH e MSS.

A partir da versão 2.0, o SPEKE está alinhado a uma versão específica do CPIX:

No lado do SPEKE, isso é imposto por meio do uso do `X-Speke-Version` cabeçalho HTTP e, no lado do CPIX, pelo uso do atributo `CPIX@version`. A falta desses elementos nas solicitações é típica dos fluxos de trabalho legados do SPEKE v1. Nos fluxos de trabalho do SPEKE v2, espera-se que o provedor de chaves processe documentos CPIX somente se ele suportar os dois parâmetros da versão.

Para obter informações detalhadas sobre o formato de troca, consulte a especificação CPIX 2.3 do DASH Industry Forum.

No geral, o SPEKE v2 traz as seguintes evoluções em comparação com o SPEKE v1:

- Todas as tags do namespace SPEKE XML estão obsoletas em favor das tags equivalentes no namespace CPIX XML
- `SPEKE:ProtectionHeader` está obsoleto e foi substituído por `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`, `SPEKE:KeyFormat` e `SPEKE:KeyFormatVersions` estão obsoletos e foram substituídos por `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id` é substituído por `CPIX@contentId`
- Novos atributos obrigatórios do CPIX: `CPIX@version`, `ContentKey@commonEncryptionScheme`
- Novo elemento CPIX opcional: `DRMSystem.ContentProtectionData`
- Suporte para várias chaves de conteúdo
- Mecanismo de versionamento cruzado entre SPEKE e CPIX
- Evolução dos cabeçalhos HTTP: novo cabeçalho `X-Speke-Version`, cabeçalho `Speke-User-Agent` renomeado para `X-Speke-User-Agent`
- Defasagem da API Heartbeat

Como a especificação SPEKE v1 permanece inalterada, as implementações existentes não precisam mudar para continuar oferecendo suporte aos fluxos de trabalho do SPEKE v1.

Tópicos

API SPEKE v2: Personalizações e restrições para a especificação do DASH-IF

A especificação CPIX 2.3 do DASH Industry Forum oferece suporte a vários casos de uso e topologias. A especificação API SPEKE v2.0 define tanto um perfil CPIX como uma API para CPIX. Para atingir esses dois objetivos, ela segue a especificação CPIX com as seguintes personalizações e restrições:

Perfil do CPIX

- O SPEKE segue o fluxo de trabalho de criptografador e consumidor.
- Para chaves de conteúdo criptografadas, o SPEKE aplica as seguintes restrições:
  - O SPEKE não oferece suporte à verificação de assinatura digital (XMLDSIG) para cargas de solicitação ou resposta.
  - O SPEKE exige 2048 certificados baseados em RSA.
- O SPEKE aproveita apenas um subconjunto das funcionalidades do CPIX:
  - O SPEKE omite a funcionalidade `UpdateHistoryItemList`. Se a lista estiver presente na resposta, o SPEKE vai ignorá-la.
  - O SPEKE omite a funcionalidade da chave raiz/folha. Se o atributo `ContentKey@dependsOnKey` estiver presente na resposta, o SPEKE vai ignorá-la.
  - O SPEKE omite o elemento `BitrateFilter` e o atributo `VideoFilter@wcg`. Se esses elementos ou atributos estiverem presentes na carga útil do CPIX, o SPEKE a ignorará.

- Somente os elementos ou atributos referenciados como “Suportados” na página Componentes de Carga Útil Padrão ou na página do contrato de criptografia podem ser usados em documentos CPIX trocados com o SPEKE v2.
- Quando incluídos em uma solicitação CPIX pelo criptografador, todos os elementos e atributos devem conter um valor válido na resposta CPIX do provedor de chaves. Caso contrário, o criptografador deve parar e gerar um erro.
- O SPEKE suporta a rotação de chaves com `KeyPeriodFilter` elementos. O SPEKE usa apenas o `ContentKeyPeriod@index` para rastrear o período chave.
- Para a sinalização HLS, vários `DRMSystem.HLSSignalingData` elementos devem ser usados: um com um valor de `DRMSystem.HLSSignalingData@playlist` atributo de 'media' e outro com um valor de `DRMSystem.HLSSignalingData@playlist` atributo de 'master'.
- Ao solicitar chaves, o criptografador pode usar o atributo opcional `@explicitIV` no elemento `ContentKey`. O provedor de chaves pode responder com um IV usando `@explicitIV`, mesmo se o atributo não estiver incluído na solicitação.
- O criptografador cria o identificador de chaves (`KID`), que permanece o mesmo para qualquer período de chave e ID de conteúdo. O provedor de chaves inclui o servidor `KID` na resposta ao documento da solicitação.
- O criptografador deve incluir um valor para o atributo `CPIX@contentId`. Ao receber um valor vazio para esse atributo, o provedor da chave deve retornar um erro com a descrição “CPIX@contentId ausente”. O valor `CPIX@contentId` não pode ser substituído pelo provedor da chave.

  O valor `CPIX@id`, se não for nulo, deve ser ignorado pelo provedor da chave.
- O criptografador deve incluir um valor para o atributo `CPIX@version`. Ao receber um valor vazio para esse atributo, o provedor da chave deve retornar um erro com a descrição “CPIX@version ausente”. Ao receber uma solicitação com uma versão não compatível, a descrição do erro retornada pelo provedor da chave deve ser “CPIX@version não compatível”.

  O valor `CPIX@version` não pode ser substituído pelo provedor da chave.
- O criptografador deve incluir um valor para o atributo `ContentKey@commonEncryptionScheme` para cada chave solicitada. Ao receber um valor vazio para esse atributo, o provedor da chave retornará um erro com a descrição “Missing ContentKey @ commonEncryptionScheme for KIDid”.

  Um documento CPIX exclusivo não pode misturar vários valores para atributos `ContentKey@commonEncryptionScheme` diferentes. Ao receber essa combinação, o

provedor da chave deve retornar um erro com a descrição “Não compatível ContentKey @ commonEncryptionScheme combinação”.

Nem todos os valores `ContentKey@commonEncryptionScheme` são compatíveis com todas as tecnologias DRM. Ao receber essa combinação, o provedor da chave deve retornar um erro com a descrição 'ContentKey@ commonEncryptionScheme não compatível com o sistema DRMid'.

O valor `ContentKey@commonEncryptionScheme` não pode ser substituído pelo provedor da chave.

- Ao receber valores diferentes para `DRMSystem@PSSH` e elemento `DRMSystem.ContentProtectionData` innerXML `<pssh>` no corpo da resposta CPIX, o criptografador deve parar e gerar um erro.

API para CPIX

- O provedor da chave deve incluir um valor para o cabeçalho da resposta `X-Speke-User-Agent` HTTP.
- O criptografador em conformidade com o SPEKE atua como um cliente e envia operações ao endpoint do provedor de chaves.
- O criptografador deve incluir um valor para o cabeçalho da solicitação `X-Speke-Version` HTTP, com a versão SPEKE usada com a solicitação, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0. Se o provedor da chave não for compatível com a versão SPEKE usada pelo criptografador para a solicitação atual, ele retornará um erro com a descrição “Versão SPEKE não compatível” e não tentará processar o documento CPIX da melhor maneira possível.

  O valor do cabeçalho `X-Speke-Version` definido pelo criptografador não pode ser modificado pelo provedor da chave na resposta à solicitação.
- Ao receber erros no corpo da resposta, o criptografador deve gerar um erro e não repetir a solicitação com um versionamento do SPEKE v1.0.

  Se o provedor da chave não retornar um erro, mas falhar em retornar um documento CPIX que inclua as informações obrigatórias, o criptografador deverá parar e gerar um erro.

A tabela a seguir resume as mensagens padrão que devem ser retornadas pelo provedor da chave no corpo da mensagem. O código de resposta HTTP em casos de erro deve ser 4XX ou 5XX, nunca 200. O código de erro 422 pode ser usado para todos os erros relacionados ao SPEKE/CPIX.

Caso de erro	Mensagem de erro
CPIX@contentId não está definido	CPIX@contentId ausente
CPIX@version não está definido	CPIX@version ausente
CPIX@version não é suportado	CPIX@version não compatível
ContentKey@ não commonEncryptionScheme está definido	Falta ContentKey @ commonEncryptionScheme para KID `id` (onde `id` é igual ao valor ContentKey @kid)
Vários commonEncryptionScheme valores ContentKey @ usados em um único documento CPIX	Combinação ContentKey @ commonEncryptionScheme não compatível
ContentKey@ não commonEncryptionScheme é compatível com a tecnologia DRM	ContentKey@ commonEncryptionScheme não compatível com DRMSystem `id` (onde é `id` igual ao valor DRMsystem @systemId)
O valor do cabeçalho X-Speke-Version não está em uma versão SPEKE compatível	Versão de SPEKE não compatível
O contrato de criptografia está malformado	Contrato de criptografia malformado
O contrato de criptografia contradiz as restrições dos níveis de segurança do DRM	O contrato de criptografia CPIX solicitado não é compatível
O contrato de criptografia não inclui VideoFilter nenhum AudioFilter elemento	Contrato de criptografia CPIX ausente

API SPEKE v2: Componentes de carga útil padrão

Por meio de uma única solicitação SPEKE, o criptografador pode solicitar várias chaves de conteúdo, juntamente com a sinalização de manifestação necessária para vários formatos de empacotamento, de acordo com o contrato de criptografia definido para um determinado conteúdo.

Para cobrir todos esses aspectos, um documento CPIX padrão é composto por três seções de lista obrigatórias, além de uma seção de lista opcional para rotação de chaves de conteúdo em tempo real.

<cpix:CPIX><cpix: ContentKeyList > seção e elemento de nível superior

Esta é uma seção obrigatória, relevante para streaming ao vivo e VOD, definindo as diferentes chaves de conteúdo que precisam ser usadas pelo criptografador. O elemento `<cpix:ContentKeyList>` pode conter um ou vários elementos `<cpix:ContentKey>` secundários, cada um deles descrevendo uma chave de conteúdo distinta.

De acordo com a especificação CPIX, os valores possíveis do atributo `ContentKey@commonEncryptionScheme` são definidos na especificação Criptografia comum em arquivos de formato de mídia base ISO (ISO/IEC 23001-7:2016):

- 'cenc': amostra completa do modo AES-CTR e criptografia de subamostra NAL de vídeo
- 'cbc1': amostra completa do modo AES-CBC e criptografia de subamostra NAL de vídeo
- 'cens': criptografia parcial de padrão NAL de vídeo no modo AES-CTR
- 'cbcs': criptografia parcial de padrão NAL de vídeo no modo AES-CBC

O exemplo a seguir mostra um documento CPIX com uma única chave de conteúdo não criptografada:

```
<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>
```

Por padrão, as chaves de conteúdo não são criptografadas, como no exemplo abaixo. Mas a criptografia das chaves de conteúdo pode ser solicitada pelo criptografador por meio da inclusão do

elemento<cpix : >. DeliveryDataList Consulte a seção Criptografia de chave de conteúdo para obter mais detalhes.

Elemento suportado pelo SPEKE	Atributos obrigatórios	Atributos opcionais	Elementos secundários obrigatórios	Elementos secundários opcionais
<cpix:CPIX>	contentId , version, xmlns:cpix, xmlns:pskc	name, xmlns:enc	um <cpix: ContentKeyList >, um<cpix : DRM >, um <cpix: SystemLis t > ContentKe yUsageRuleList	um <cpix: DeliveryDataList >, um <cpix : >ContentK eyPeriodList
<clix : >ContentK eyList	-	id	pelo menos um <cpix : >ContentKey	-
<clix : >ContentK ey	criança commonEnc ryptionScheme, Dados	id, Algorithm, explicitIV	um <pskc:Sec ret>	-
<pskc:Secret>	PlainValue ou EncryptedValue	ValueMAC	-	<enc: Encryptio nMethod >, <enc : >CipherData

SystemList<CPIX:DRM >seção

Esta é uma seção obrigatória, relevante para streaming ao vivo e VOD, definindo os diferentes sistemas DRM que precisam ser aproveitados junto com as chaves de conteúdo.

O exemplo a seguir mostra uma lista de sistemas DRM com uma única especificação de sistema PlayReady DRM:

```
<cpix:DRMSystemList>
```

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

Para obter uma lista completa de systemIDs DRM, consulte a seção Proteção de Conteúdo do repositório de identificadores DASH-IF.

Elemento suportado pelo SPEKE	Atributos obrigatórios	Atributos opcionais	Elementos secundários obrigatórios	Elementos secundários opcionais
<CPIX : DRM >SystemList	-	id	pelo menos um <cpix:DRM System>	-
<cpix:DRM System>	kid, systemId	id, name, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHeaderData, dois <Cpix:HLSSignalingData> elementos com valores de atributo de playlist diferentes

`DRMSystem@PSSH` é obrigatório se o encapsulamento ISO-BMFF for aplicado a segmentos de mídia. O elemento `DRMSystem.ContentProtectionData` innerXML `<pssh>` é utilizado pelo criptografador somente para fins de sinalização de manifesto.

Se `DRMSystem@PSSH` estiver presente e `DRMSystem.ContentProtectionData` contiver um `<pssh>` elemento innerXML, ambos os valores devem ser idênticos.

Se a sinalização `DRMSystem` deve ser transmitida em manifestos HLS, ambos os elementos `<cpix:HLSSignalingData playlist="media">` e `<cpix:HLSSignalingData playlist="master">` devem ser incluídos na solicitação e na resposta do CPIX.

<cpix : **>**seção ContentKeyPeriodList

Essa é uma seção opcional, relevante somente para transmissão em tempo real, que define os períodos criptográficos aplicados ao conteúdo.

O elemento `<cpix:ContentKeyPeriodList>` pode conter um ou vários elementos `<cpix:ContentKeyPeriod>` secundários, cada um deles descrevendo uma chave de conteúdo distinta. Usar UUIDs como parte do valor do atributo id é uma abordagem comumente usada.

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

Elemento suportado pelo SPEKE	Atributos obrigatórios	Atributos opcionais	Elementos secundários obrigatórios	Elementos secundários opcionais
<clix : **>**ContentKeyPeriodList	-	id	pelo menos um **<**cpix : **>**ContentKeyPeriod	-
<clix : **>**ContentKeyPeriod	id, index	-	-	-

Se forem usados períodos criptográficos, as chaves de criptografia também precisarão ser anexadas a um dos períodos criptográficos no documento CPIX, conforme mostrado na seção abaixo.

<cpix : >seção ContentKeyUsageRuleList

Esta é uma seção obrigatória, relevante para streaming ao vivo e VOD, que define como as diferentes chaves de conteúdo protegerão as faixas dentro do streamset e durante os períodos criptográficos.

O elemento <cpix: ContentKeyUsageRuleList > pode conter um ou vários elementos secundários <cpix: ContentKeyUsageRule >, cada um deles descrevendo as faixas às quais uma determinada chave de conteúdo é aplicada pelo criptografador, potencialmente durante um período criptográfico específico. É necessário que pelo menos um elemento <cpix: AudioFilter > ou um <cpix: VideoFilter > esteja presente em um elemento<cpix : >. ContentKeyUsageRule

O exemplo a seguir mostra uma lista simples com apenas uma regra aplicando uma única chave de conteúdo a todas as faixas de áudio e vídeo durante um período criptográfico 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 suportado pelo SPEKE	Atributos obrigatórios	Atributos opcionais	Elementos secundários obrigatórios	Elementos secundários opcionais
<clix : >ContentKeyUsageRuleList	-	id	pelo menos um <cpix : >ContentKeyUsageRule	-
<clix : >ContentKeyUsageRule	criança, intendedTrackType	-	pelo menos um <cpix: AudioFilter > ou um <cpix : >(*) VideoFilter	<clix : >KeyPeriodFilter

Elemento suportado pelo SPEKE	Atributos obrigatórios	Atributos opcionais	Elementos secundários obrigatórios	Elementos secundários opcionais
<clix : >KeyPeriodFilter	periodId	-	-	-
<clix : >AudioFilter	-	minChannels, maxChannels	-	-
<clix : >VideoFilter	-	minPixels, maxPixels, hdr, minFps, maxFps	-	-

(*) Para obter uma explicação detalhada sobre o uso de uma ou várias chaves de conteúdo para proteger uma ou várias faixas em um streamset, consulte a seção Documentação do Contrato de Criptografia.

API SPEKE v2: Contrato de criptografia

O contrato de criptografia define quais chaves de conteúdo estão protegendo quais faixas dentro de um determinado streamset, com base nas características das faixas.

O uso de várias chaves de conteúdo para faixas diferentes em um streamset, apesar de ser uma prática recomendada do setor, não é obrigatório, mas recomendado: pelo menos duas chaves de conteúdo diferentes, uma para faixas de áudio e outra para faixas de vídeo. É possível usar uma única chave de conteúdo para criptografar várias faixas, mas isso precisa ser explicitamente sinalizado no documento CPIX enviado pelo criptografador ao provedor da chave. De um modo geral, o criptografador sempre descreve com precisão quantas chaves de conteúdo são necessárias e como elas são usadas para criptografar as várias faixas de mídia.

Princípios

O contrato de criptografia está localizado na `<cpix:ContentKeyUsageRuleList>` seção do documento CPIX. Nesta seção, cada chave de conteúdo definida na `<cpix:ContentKeyList>` seção corresponde a um `<cpix:ContentKeyUsageRule>` elemento específico, que deve incluir:

- um `ContentKeyUsageRule@intendedTrackType` atributo que pode referenciar um ou mais subcomponentes, separados pelo sinal '+' se vários subcomponentes forem usados. O valor

de `ContentKeyUsageRule@intendedTrackType` deve ser exclusivo em um contrato de criptografia e não pode ser usado em múltiplos elementos `ContentKeyUsageRule`.

- Um ou mais elementos `<cpix:AudioFilter>` ou elemento `<cpix:VideoFilter>` secundário, dependendo do valor do `ContentKeyUsageRule@intendedTrackType` atributo.

As regras que regem esse relacionamento são as seguintes:

- Quando todas as faixas de áudio e vídeo do streamset precisarem ser protegidas com uma chave de conteúdo exclusiva, a string `'ALL'` deve ser usada como valor do atributo `ContentKeyUsageRule@intendedTrackType`. O exemplo 1 mostra esse caso de uso. Nesta situação, elementos `<cpix:AudioFilter />` e `<cpix:VideoFilter />` secundários sem nenhum atributo devem ser incluídos. Qualquer outra combinação de `<cpix:AudioFilter>` e/ou `<cpix:VideoFilter>` elementos é inválida nesse contexto específico.
- Para todos os outros casos de uso, o valor do atributo `ContentKeyUsageRule@intendedTrackType` pode ser definido livremente, e o número de elementos `<cpix:AudioFilter />` e `<cpix:VideoFilter />` secundários devem corresponder ao número de subcomponentes agregados por meio do sinal “+”. Os exemplos 2/3/4/5/6/7/9/10 ilustram esse requisito, quando um único subcomponente está presente no valor do atributo `ContentKeyUsageRule@intendedTrackType`. O exemplo 8 ilustra isso quando vários subcomponentes são usados: `ContentKeyUsageRule@intendedTrackType="SD +HD"` é descrito por dois elementos `<cpix:VideoFilter>` secundários distintos com valores de atributos diferentes e `ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"` é descrito por três elementos `<cpix:VideoFilter>` secundários distintos com valores de atributos diferentes.

Filtros

O CPIX define vários elementos e atributos de filtragem, mas o SPEKE suporta apenas um subconjunto deles. A tabela a seguir resume essas diferenças:

Tipo de filtro CPIX	Suporte geral do SPEKE	Atributos de filtro suportados pelo SPEKE	Atributos de filtro não suportados pelo SPEKE
<clix : >VideoFilter	Sim	minPixels, maxPixels, hdr, minFPS, maxFPS (atributos opcionais)	wcg
<clix : >AudioFilter	Sim	minChannels, maxChannels (atributos opcionais)	
<clix : >KeyPerio dFilter	Sim	periodId (atributo obrigatório)	
<clix : >BitrateFilter	Não	N/D	N/D
<clix : >LabelFilter	Não	N/D	N/D

De acordo com a especificação CPIX para VideoFilter, [minPixels, maxPixels] é um intervalo com tudo incluído em ambas as dimensões, enquanto (minFPS, maxFPS] é inclusivo somente para a dimensão maxFPS. Pois AudioFilter, [minChannels, maxChannels] é um intervalo inclusivo em ambas as dimensões.

Situações problemáticas

Há situações em que as informações fornecidas no contrato de criptografia podem ser parciais, ambíguas ou errôneas. Nesses casos, é importante que o criptografador e o provedor da chave se comportem adequadamente e garantam a proteção adequada do conteúdo. A tabela a seguir apresenta o comportamento recomendado nessas situações:

Nessa situação	O criptografador deve...	O provedor da chave deve...
Nenhuma regra se aplica a uma ou mais faixas no streamset (veja o exemplo 3 abaixo)	O criptografador deve examinar sua configuração (externa à carga útil do CPIX) e verificar se as faixas em questão não exigem criptogra	Não relevante: o provedor da chave não tem conhecimento da estrutura do streamset.

Nessa situação	O criptografador deve...	O provedor da chave deve...
	fia. Se não corresponder à expectativa, o criptografador deve gerar um erro e interromper o processamento.	
Várias regras se sobrepõem e sugerem várias chaves de conteúdo para criptografar uma faixa específica	O criptografador deve aplicar a última avaliação ContentKeyUsageRule bem-sucedida na ordem do documento.	Não relevante: o provedor da chave não tem conhecimento da estrutura do streamset.
O contrato de criptografia muda em um único ciclo de solicitação/resposta do SPEKE	O criptografador deve levantar uma exceção e interromper o processamento, pois o provedor da chave não é responsável pela definição do contrato de criptografia.	Para evitar que essa situação ocorra em primeiro lugar, o provedor da chave não deve modificar um contrato de criptografia recebido na carga útil CPIX da solicitação SPEKE.
Contrato de criptografia malformado: intendedTrackType /Filters, exceção de restrição de cardinalidade, filtros ou atributos não suportados	O criptografador deve gerar uma exceção, interromper o processamento e não enviar a solicitação SPEKE ao provedor da chave, pois isso provavelmente resultaria em proteção de conteúdo incorreta ou deixaria alguns rastros desprotegidos.	O provedor da chave deve gerar uma exceção e retornar um erro de “contrato de criptografia malformado”.

Nessa situação	O criptografador deve...	O provedor da chave deve...
Contrato de criptografia bem-formado, mas que viole as restrições dos níveis de segurança do DRM: por exemplo, uma única chave de conteúdo sendo solicitada para proteger as faixas de áudio e as faixas de vídeo UHD	Se o criptografador tiver conhecimento das restrições dos níveis de segurança do DRM, ele deve gerar uma exceção, interromper o processamento e não enviar a solicitação SPEKE ao provedor da chave, pois isso provavelmente resultaria em proteção de conteúdo incorreta.	O provedor da chave deve gerar uma exceção e retornar um erro de “contrato requisitado de criptografia CPIX não compatível”.
Contrato de criptografia ausente	O criptografador não deve enviar documentos CPIX que não contenham nenhum VideoFilter elemento ou. AudioFilter	O provedor da chave deve gerar uma exceção e retornar um erro de “contrato de criptografia CPIX ausente”.

Exemplos de contratos de criptografia

Exemplo 1: uma chave de conteúdo para todas as faixas de áudio e 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>
```

Exemplo 2: uma chave de conteúdo para todas as faixas de vídeo, uma chave de conteúdo para todas as faixas de áudio

```
<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>
```

Exemplo 3: uma chave de conteúdo para todas as faixas de vídeo e faixas de áudio não criptografadas

```
<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>
```

Exemplo 4: várias chaves de conteúdo para diferentes faixas de vídeo (SD/HD), uma chave de conteúdo para todas as faixas de áudio

```
<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>
```

Exemplo 5: várias chaves de conteúdo para diferentes faixas de vídeo (SD/HD/UHD), uma chave de conteúdo para todas as faixas de áudio

```
<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>
```

Exemplo 6: várias chaves de conteúdo para diferentes faixas de vídeo (SD/HD/UHD1/UHD2), uma chave de conteúdo para todas as faixas de áudio

```
<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>
```

Exemplo 7: várias chaves de conteúdo para diferentes faixas de vídeo (SD/HD1/HD2/UHD1/UHD2), uma chave de conteúdo para todas as faixas de áudio

```
<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>
```

Exemplo 8: várias chaves de conteúdo para diferentes faixas de vídeo (baseadas em múltiplos tipos de atributos), uma chave de conteúdo para todas as faixas de áudio

```
<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>
```

Exemplo 9: uma chave de conteúdo para todas as faixas de vídeo, várias chaves de conteúdo para faixas de áudio estéreo e 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>
```

Exemplo 10: uma chave de conteúdo para todas as faixas de vídeo, várias chaves de conteúdo para estéreo e dois tipos de faixas de áudio 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>
```

API SPEKE v2: Exemplos de chamadas de método de fluxo de trabalho em tempo real

Exemplo de sintaxe de solicitação

O seguinte URL é um exemplo e não indica um formato fixo:

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

Corpo da solicitação

Um documento CPIX.

Cabeçalhos de solicitação

Nome	Tipo	Ocorre	Descrição
`AWS Authorization`	Cadeia de caracteres	1..1	Consulte AWS Sigv4
`X-Amz-Security-Token`	String	1..1	Consulte AWS Sigv4
`X-Amz-Date`	String	1..1	Consulte AWS Sigv4
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	Versão da API SPEKE usada com a solicitação, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Cabeçalhos de resposta

Nome	Tipo	Ocorre	Descrição
`X-Speke-User-Agent`	Cadeia de caracteres	1..1	String que identifica o provedor de chaves
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	Versão da API SPEKE usada com a solicitação, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Resposta de solicitação

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`200 (Success)`	CPIX	1..1	Resposta da carga DASH-CPIX:
`4XX (Client error)`	Mensagem de erro do cliente	1..1	Descrição do erro do cliente
`5XX (Server error)`	Mensagem de erro do servidor	1..1	Descrição de erro do servidor

> **Note**
>
> Os exemplos nesta seção não incluem a criptografia de chaves de conteúdo. Para obter informações sobre como adicionar criptografia de chaves de conteúdo, consulte Criptografia de chaves de conteúdo.

Exemplo de carga de solicitação em tempo real com chaves em branco

O exemplo a seguir mostra uma carga útil típica de solicitação ao vivo do criptografador para o provedor da chave DRM, com uma chave de conteúdo para todas as faixas de vídeo e uma chave de conteúdo para todas as faixas de áudio:

```
<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>
```

Exemplo de carga de resposta em tempo real com chaves em branco

O exemplo a seguir mostra uma carga útil de resposta típica do provedor de chaves DRM (os valores retornados foram encurtados com [...] para facilitar a leitura):

```
<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>
```

API SPEKE v2: Exemplos de chamadas de método de fluxo de trabalho de VOD

Exemplo de sintaxe de solicitação

O seguinte URL é um exemplo e não indica um formato fixo.

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

Corpo da solicitação

Um documento CPIX.

Cabeçalhos de solicitação

Nome	Tipo	Ocorre	Descrição
`AWS Authorization`	Cadeia de caracteres	1..1	Consulte AWS Sigv4
`X-Amz-Security-Token`	String	1..1	Consulte AWS Sigv4
`X-Amz-Date`	String	1..1	Consulte AWS Sigv4

Nome	Tipo	Ocorre	Descrição
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	Versão da API SPEKE usada com a solicitação, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Cabeçalhos de resposta

Nome	Tipo	Ocorre	Descrição
`X-Speke-User-Agent`	Cadeia de caracteres	1..1	String que identifica o provedor de chaves
`Content-Type`	String	1..1	application/xml
`X-Speke-Version`	String	1..1	Versão da API SPEKE usada com a solicitação, formulada como. MajorVersion MinorVersion, como '2.0' para SPEKE v2.0

Resposta de solicitação

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`200 (Success)`	CPIX	1..1	Resposta da carga DASH-CPIX:
`4XX (Client error)`	Mensagem de erro do cliente	1..1	Descrição do erro do cliente

CÓDIGO HTTP	Nome da carga	Ocorre	Descrição
`5XX (Server error)`	Mensagem de erro do servidor	1..1	Descrição de erro do servidor

> **Note**
>
> Os exemplos nesta seção não incluem a criptografia de chaves de conteúdo. Para obter informações sobre como adicionar criptografia de chaves de conteúdo, consulte Criptografia de chaves de conteúdo.

Exemplo de carga de solicitação de VOD com chaves em branco

O exemplo a seguir mostra uma carga útil típica de solicitação VOD do criptografador para o provedor da chave DRM, com uma chave de conteúdo para todas as faixas de vídeo e uma chave de conteúdo para todas as faixas de áudio:

```
<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>
```

Exemplo de carga de resposta de VOD com chaves em branco

O exemplo a seguir mostra uma carga útil de resposta típica do provedor de chaves DRM (os valores retornados foram encurtados com [...] para facilitar a leitura):

```
<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>
```

API SPEKE v2: Criptografia de chave de conteúdo

Também é possível adicionar a criptografia de chaves de conteúdo à sua implementação do SPEKE. A criptografia da chave de conteúdo garante end-to-end proteção total ao criptografar as chaves de conteúdo para trânsito, além de criptografar o próprio conteúdo. Se não a implementar no seu provedor de chaves, dependerá apenas da criptografia de camada de transporte e da forte autenticação para segurança.

Para usar a criptografia de chaves de conteúdo em criptografadores executados na Nuvem AWS, clientes importam certificados para o AWS Certificate Manager e, depois, usam os ARNs do certificado resultante nas atividades de criptografia. O criptografador usa os ARNs dos certificados e o serviço do ACM para fornecer chaves de conteúdo criptografadas para o provedor de chaves de DRM.

Restrições

O SPEKE oferece suporte à criptografia de chaves de conteúdo, conforme detalhado na especificação CPIX do DASH-IF, com as seguintes restrições:

- O SPEKE não oferece suporte à verificação de assinatura digital (XMLDSIG) para cargas de solicitação ou resposta.
- O SPEKE exige 2048 certificados baseados em RSA.

Essas restrições também estão listadas em Personalizações e restrições à especificação DASH-IF.

Implementar a criptografia de chaves de conteúdo

Para oferecer a criptografia de chaves de conteúdo, inclua o seguinte em suas implementações do provedor de chaves DRM:

- Gerencie o elemento `<cpix:DeliveryDataList>` nas cargas de solicitação e de resposta.
- Forneça valores criptografados em `<cpix:ContentKeyList>` das cargas de resposta.

Para obter mais informações sobre esses elementos, consulte a Especificação do DASH-IF CPIX 2.3.

Exemplo de elemento de criptografia de chaves de conteúdo `<cpix:DeliveryDataList>` na carga de solicitação

```
<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>
```

Exemplo de elemento de criptografia de chaves de conteúdo `<cpix:DeliveryDataList>` na carga de resposta

```
<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>
```

Exemplo de elemento de criptografia de chaves de conteúdo `<cpix:ContentKeyList>` na carga de resposta

O exemplo a seguir mostra o tratamento das chaves de conteúdo criptografadas no elemento `<cpix:ContentKeyList>` da carga de resposta. O elemento `<pskc:EncryptedValue>` é usado:

```
<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>
```

Por comparação, o exemplo a seguir mostra uma carga de resposta semelhante à chave de conteúdo entregue sem criptografia, como uma chave em branco. O elemento `<pskc:PlainValue>` é usado:

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

SPEKE API v2: Substituindo o identificador de chave

O criptografador cria um novo identificador de chave (KID) sempre que ele alterna chaves. Ele repassa o KID para o provedor de chaves de DRM nas solicitações. Quase sempre, o provedor de chaves responde usando o mesmo KID, mas pode fornecer um valor diferente para o KID na resposta.

O seguinte é uma solicitação de exemplo com o 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>
```

A seguinte resposta substitui o KID por `22222222-2222-2222-2222-222222222222`:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
 kid="22222222-2222-2222-2222-222222222222" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- Widevine -->
  <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
```

```
    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>
   <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
  index="1" />
  </cpix:ContentKeyPeriodList>
  <cpix:ContentKeyUsageRuleList>
   <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222"
  intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
   </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Licença

Atribuição Creative Commons - Licença Pública Internacional ShareAlike 4.0

Ao exercer os Direitos Licenciados (definidos abaixo), Você aceita e concorda em se comprometer com os termos e condições desta Licença Pública Internacional Creative Commons ShareAlike Atribuição-4.0 (“Licença Pública”). Na medida em que esta licença pode ser interpretada como um contrato, são concedidos a Você Direitos Licenciados em vista de sua aceitação destes termos e condições. Além disso, o Licenciante concede esses direitos a Você em vista dos benefícios que ele recebe ao disponibilizar o Material Licenciado de acordo com esses termos e condições.

Seção 1 – Definições.

a. Material Adaptado significa material sujeito a Direitos Autorais e Direitos Conexos que é derivado ou baseado em Material Licenciado e no qual o Material Licenciado é traduzido, alterado, organizado, transformado ou modificado de um modo que exige permissão segundo os Direitos Autorais e Direitos Conexos mantidos pelo Licenciante. Para a finalidade desta Licença Pública, quando o Material Licenciado é uma obra musical, performance ou gravação musical, sempre se produz um Material Adaptado quando esse material é submetido a uma sincronização cronometrada em relação a uma imagem em movimento.

b. Licença do Adaptador refere-se à licença que Você aplica aos Direitos Autorais e Direitos Conexos em suas contribuições para o Material Adaptado, de acordo com os termos e condições da Licença Pública.

c. Licença compatível com BY-SA significa uma licença listada em creativecommons.org/compatiblelicenses, aprovada pela Creative Commons como essencialmente equivalente a esta Licença Pública.

d. Direitos Autorais e Direitos Conexos (ou Similares) referem-se a direitos autorais e/ou a direitos similares estreitamente relacionadas com direitos autorais e que incluem, entre outros, performance, transmissão, gravação musical e Direitos de Banco de Dados Sui Generis, independentemente da forma como os direitos são chamados ou categorizados. Para a finalidade desta Licença Pública, os direitos especificados na Seção 2(b)(1)-(2) não são Direitos Autorais e Direitos Conexos.

e. Medidas Tecnológicas Efetivas referem-se a medidas que, na ausência de autoridade apropriada, não podem ser burladas segundo a lei que satisfaça às obrigações prescritas no artigo 11 do Tratado de Direitos Autorais da WIPO, adotado em 20 de dezembro de 1996, e/ou acordos internacionais semelhantes.

f. Exceções e Limitações significam uso legítimo, negociação justa e/ou qualquer outra exceção ou limitação aos Direitos Autorais e Direitos Conexos que se aplicam ao uso que Você faz do Material Licenciado.

g. Elementos de licença significam os atributos da licença listados no nome de uma Licença Pública Creative Commons. Os elementos de licença desta Licença Pública são Atribuição e. ShareAlike

h. Material Licenciado refere-se a obra artística ou literária, banco de dados ou outro material ao qual o Licenciante aplica esta Licença Pública.

i. Direitos Licenciados referem-se a direitos concedidos a Você que estão sujeitos aos termos e condições desta Licença Pública, os quais estão limitados a todos os Direitos Autorais e Direitos Conexos que se aplicam ao uso que Você faz do Material Licenciado e que o Licenciante tem autoridade para licenciar.

j. Licenciante refere-se ao(s) indivíduo(s) ou à(s) entidade(s) que concedem direitos sob esta Licença Pública.

k. Compartilhar significa fornecer material ao público por qualquer meio ou processo que requer permissão de acordo com os Direitos Licenciados, como reprodução pública, exibição pública, performance pública, distribuição, disseminação, comunicação ou importação, e disponibilizar material ao público de uma forma que ele possa acessá-lo material de um local e em um momento individualmente escolhidos por eles.

l. Direitos de Banco de Dados Sui Generis referem-se a outros direitos além dos direitos autorais, resultantes da Diretiva 96/9/CE do Parlamento Europeu e do Conselho de 11 março de 1996, sobre proteção legal de bancos de dados, tal como for emendado e/ou substituído, bem como outros direitos essencialmente equivalentes em qualquer lugar do mundo.

m. Você significa o indivíduo ou a entidade que exerce os Direitos Licenciados sob esta Licença Pública. Seu tem um significado correspondente.

Seção 2 – Escopo.

a. Concessão de licença.

1. De acordo com os termos e condições desta Licença Pública, por meio deste documento o Licenciante concede a Você uma licença de abrangência mundial, isenta de royalties, não sublicenciável, não exclusiva e irrevogável para exercer os Direitos Licenciados no Material Licenciado para:

   A. A. reproduzir e compartilhar o Material Licenciado, no todo ou em parte; e

   B. B. produzir, reproduzir e compartilhar material adaptado.

2. Exceções e limitações. Para evitar dúvidas, nos casos em que as Exceções e Limitações se aplicam ao seu uso, essa Licença Pública não se aplica, e Você não precisa estar em conformidade com os respectivos termos e condições.

3. Período de vigência. A duração desta Licença Pública é especificada na Seção 6(a).

4. Mídias e formatos; modificações técnicas permitidas. O Licenciante autoriza Você a exercer os Direitos Licenciados em todos os formatos e mídias, sejam eles conhecidos agora ou concebidos futuramente, e a realizar as modificações técnicas necessárias para fazê-lo. O Licenciante renuncia e/ou concorda em não reivindicar qualquer direito ou autoridade a fim de proibir Você de fazer as modificações técnicas necessárias para exercer os Direitos Licenciados, inclusive as modificações técnicas necessárias para contornar Medidas Tecnológicas Efetivas. Para a finalidade desta Licença Pública, as modificações autorizadas realizadas conforme esta Seção 2(a)(4) nunca constituirão Material Adaptado.

5. Destinatários posteriores.

   A. Proposta do Licenciante – Material Licenciado. Todo destinatário do Material Licenciado receberá automaticamente uma proposta do Licenciante para exercer os Direitos Licenciados de acordo com os termos e condições desta Licença Pública.

   B. Oferta adicional do Licenciante — Material Adaptado. Cada destinatário do Material Adaptado de Você recebe automaticamente uma oferta do Licenciador para exercer os

Direitos Licenciados no Material Adaptado sob as condições da Licença do Adaptador que Você aplica.

C. Nenhuma restrição posterior. Você não pode propor ou impor nenhum outro termo ou condição diferente ou aplicar qualquer Medida Tecnológica Efetiva ao Material, se isso restringir o exercício dos Direitos Licenciados por qualquer destinatário do Material Licenciado.

6. Nenhum endosso. Nada nesta Licença Pública constitui ou pode ser interpretado como permissão para declarar ou sugerir que Você está associado – ou que o uso que Você faz do Material Licenciado está associado é patrocinado, endossado ou recebeu status oficial – com o Licenciante ou outros designados para receber atribuição, tal como estabelecido na Seção 3(a)(1)(A)(i).

b. Outros direitos.

1. Os direitos morais, como o direito de integridade, não são licenciados sob esta Licença Pública, nem o são os direitos de publicidade, privacidade e/ou outros direitos semelhantes de personalidade; no entanto, na medida do possível, o Licenciante renuncia e/ou concorda em não reivindicar nenhum direito por ele mantido, na proporção máxima necessária para que Você exerça os Direitos Licenciados, mas não o contrário.
2. Os direitos de patentes e marca comercial não são licenciados sob esta Licença Pública.
3. Na medida do possível, o Licenciante renuncia a qualquer direito de recolher royalties de Você pelo exercício dos Direitos Licenciados, seja diretamente ou por meio de uma sociedade de recolhimento, sob qualquer esquema de licenciamento estatutário ou compulsório voluntário ou renunciável. Em todos os outros casos, o Licenciante reserva-se expressamente o direito de recolher esses royalties.

Seção 3 – Condições de licença.

O exercício dos Direitos Licenciados está expressamente sujeito às condições a seguir.

a. Atribuição.

1. Se Você compartilhar o Material Licenciado (incluindo sua forma modificada), deverá:

A. A. reter o seguinte, se fornecido pelo Licenciante com o Material Licenciado;

```
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. B. indicar se Você modificou o Material Licenciado e manter uma indicação de quaisquer modificações anteriores; e

C. C. indicar que o Material Licenciado é licenciado de acordo com esta Política Pública e incluir o texto ou o URL ou hiperlink desta Licença Pública.

2. Você pode satisfazer as condições na Seção 3(a)(1), de qualquer forma razoável, com base na mídia, nos meios e no contexto em que Você compartilhar o Material Licenciado. Por exemplo, pode ser cabível satisfazer as condições ao fornecer um URI ou hiperlink para um recurso que inclui as informações necessárias.
3. Se solicitado pelo Licenciante, Você deve remover qualquer uma das informações requeridas pela Seção 3(a)(1)(A), se razoavelmente viável.

b. ShareAlike. Além das condições na Seção 3(a), se você compartilhar material adaptado que você produz, as seguintes condições também se aplicam.

1. A Licença do Adaptador que você aplica deve ser uma licença Creative Commons com os mesmos Elementos de Licença, esta versão ou posterior, ou uma Licença compatível com BY-SA.
2. Você deve incluir o texto, o URL ou o hiperlink da Licença do Adaptador que você aplica. Você pode satisfazer essas condições de qualquer forma razoável, com base na mídia, nos meios e no contexto em que você compartilhar o Material Adaptado.
3. Você não pode oferecer ou impor quaisquer termos ou condições adicionais ou diferentes ou aplicar quaisquer Medidas Tecnológicas Eficazes ao Material Adaptado que restrinjam o exercício dos direitos concedidos pela Licença do Adaptador que você aplica.

Seção 4 – Direitos de Banco de Dados Sui Generis.

Circunstância em que os Direitos Licenciados incluem Direitos de Banco de Dados Sui Generis que se aplicam ao uso que Você faz do Material Licenciado:

a. a. para evitar dúvidas, a Seção 2(a)(1) concede a Você o direito de extrair, reutilizar, reproduzir e compartilhar todo o conteúdo ou uma parte substancial do conteúdo do banco de dados;

b. b. se Você incluir todo ou uma parte substancial do conteúdo do banco de dados em um banco de dados em que Você tenha Direitos de Banco de Dados Sui Generis, esse banco de dados (mas não seu conteúdo específico) será considerado Material Adaptado, incluso se for pelos propósitos da Seção 3(b); e

c. Você deve cumprir as condições na Seção 3(a) se compartilhar todo ou uma parte substancial do conteúdo do banco de dados. Para evitar dúvidas, a Seção 4 complementa e não substitui suas obrigações nesta Licença Pública em que os Direitos Licenciados incluem outros Direitos Autorais e Direitos Conexos.

Seção 5 – Exclusão de garantias e limitação de responsabilidade.

a. A menos que de outra forma garantido separadamente pelo Licenciante, desde que possível, o Licenciante oferece o Material Licenciado no estado em que se encontra e do modo como foi disponibilizado e não faz declarações nem dá garantias de qualquer tipo a respeito do Material Licenciado, expressas, implícitas, legais ou outras. Isso inclui, entre outros fatores, título, garantias de propriedade, comercialização, adequação a uma finalidade específica, não violação, ausência de defeitos ocultos ou outros defeitos, precisão ou a presença ou ausência de erros, sejam ou não conhecidos ou detectáveis. Nas circunstâncias em que as exclusões de garantias não são permitidos no todo ou em parte, essa exclusão pode não se aplicar a Você.

b. Se possível, em hipótese alguma o Licenciante será responsabilizado perante Você com relação a qualquer teoria legal (incluindo, entre outras, negligência) ou por quaisquer danos diretos, especiais, indiretos, acidentais, consequenciais, punitivos, exemplares, ou por outras perdas, custos, despesas ou danos resultantes desta Licença Pública ou do uso do Material Licenciado, mesmo que o Licenciante tenha sido avisado da possibilidade dessas perdas, custos, despesas ou danos. Nas circunstâncias em que a limitação de responsabilidade não é permitida no todo ou em parte, essa limitação pode não se aplicar a Você.

c. A exclusão de garantias e limitação de responsabilidade apresentadas acima devem ser interpretadas na medida do possível de um modo que se aproxime ao máximo da isenção e exoneração absolutas de qualquer responsabilidade.

Seção 6 – Duração e rescisão.

a. Esta Licença Pública aplica-se pelo período de vigência dos Direitos Autorais e Direitos Conexos aqui licenciados. No entanto, se Você não agir de acordo com esta Licença Pública, seus direitos sob esta Licença Pública serão suspendidos automaticamente.
b. Quando seu direito de usar o Material Licenciado é suspendido de acordo com a Seção 6(a), ele é restabelecido:
    1. automaticamente a partir da data em que a violação é remediada, contanto que isso ocorra 30 dias depois da descoberta da violação; ou
    2. mediante restabelecimento expresso pelo Licenciante.
c. Para evitar dúvidas, a Seção 6(b) não afeta nenhum direito que o Licenciante possa ter de procurar reparar suas violações desta Licença Pública.
d. Para evitar dúvidas, o Licenciante também pode oferecer o Material Licenciado de acordo com termos ou condições diferentes ou parar de distribuir o Material Licenciado a qualquer momento; no entanto, isso não encerra esta Licença Pública.
e. As Seções 1, 5, 6, 7 e 8 subsistirão ao encerramento desta Licença Pública.

Seção 7 – Outros termos e condições.

a. O Licenciante não deve ser obrigado a cumprir quaisquer termos ou condições adicionais ou diferentes transmitidos por Você, a menos que isso seja expressamente combinado.
b. Quaisquer ajustes, entendimentos ou acordos sobre o Material Licenciado não descritos aqui são distintos e independentes dos termos e condições desta Licença Pública.

Seção 8 – Interpretação.

a. Para evitar dúvidas, esta Licença Pública não reduz, limita, restringe nem impõe condições a qualquer uso do Material Licenciado que possa ser feito legitimamente sem permissão sob esta Licença Pública, e não deve ser interpretada como tal.
b. Na medida do possível, se qualquer disposição desta Licença Pública for considerada inexigível, ela será automaticamente corrigida na medida mínima necessária para que se torne exequível. Se a disposição não puder ser corrigida, deverá ser cortada desta Licença Pública sem afetar o cumprimento dos termos e condições restantes.
c. Nenhum termo ou condição desta Licença Pública será objeto de renúncia e nenhuma indicação de falta de conformidade será consentida, a menos que expressamente aceita pelo Licenciante.

d. Nada nesta Licença Pública constitui ou deve ser interpretado como limitação ou renúncia a quaisquer privilégios e isenções que se aplicam ao Licenciante ou a Você, inclusive de processos jurídicos de qualquer jurisdição ou autoridade.

Histórico do documento

A tabela a seguir descreve as alterações na documentação do SPEKE.

SPEKE v1

Alteração	Descrição	Data
Matriz de suporte: serviços e produtos de parceiro da AWS	Foi adicionada uma nova seção para o suporte do SPEKE nos serviços e produtos de parceiro da AWS, listando os serviços da Bitmovin.	13 de janeiro de 2023
Atualizações para provedores de plataforma de DRM	Adição de links e novas informações de parceiros à lista de provedores de plataforma de DRM.	24 de janeiro de 2019
Incluir criptografadores de terceiros	Atualização na arquitetu ra e nas descrições para contabilizar criptografadores de terceiros.	20 de novembro de 2018
Criptografia de chaves de conteúdo	Adicionada a opção para criptografar chaves de conteúdo. Antes disso, o Secure Packager e o Encoder Key Exchange suportavam apenas a entrega de chaves em branco.	30 de outubro de 2018
Matriz de suporte: AWS Elemental Live	Adicionada uma matriz de suporte do AWS Elemental Live.	27 de setembro de 2018

Alteração	Descrição	Data
Componentes de carga padrão	Adicionada uma seção que define os principais elementos da carga JSON.	27 de setembro de 2018
Substituição de KID	Adicionada uma seção sobre substituições de KID por um provedor de chaves.	27 de setembro de 2018
Links corrigidos para o site do DASH-IF	Links corrigidos para o site do DASH IF para a especificação CPIX e para a página de IDs do sistema.	27 de setembro de 2018
Cópia de versão para o AWS Elemental Live	Atualização na documenta ção do SPEKE para incluir os produtos do AWS Elemental.	20 de julho de 2018
CMAF	Atualização das tabelas da matriz de suporte para serviços para incluir o Formato do aplicativo de mídia comum (CMAF).	27 de junho de 2018
Lançamento inicial	Primeira versão do Secure Packager and Encoder Key Exchange (SPEKE), uma especificação de comunicaç ão entre um criptografador de conteúdo e um provedor de chaves de DRM. O provedor de chaves DRM expõe uma API Secure Packager and Encoder Key Exchange para lidar com as solicitações de chave recebidas.	27 de novembro de 2017

SPEKE v2

Alteração	Descrição	Data
Atualizações na seção de provedores de plataforma de DRM	Foram adicionados novos parceiros qualificados à coluna SPEKE v2 da lista de fornecedores da plataforma DRM.	9 de agosto de 2023
Atualizações nas seções de exemplos de chamadas de métodos de fluxo de trabalho ao vivo e VOD	Foi adicionado o cabeçalho de resposta X-Speke-V ersion ausente nas seções de exemplos de chamadas do método de fluxo de trabalho SPEKE v2 ao vivo e VOD.	13 de janeiro de 2023
Atualizações na seção de provedores de plataforma de DRM e de contrato de criptografia	Foram adicionados novos parceiros qualificados à coluna SPEKE v2 da lista de fornecedores da plataform a DRM. Foram adicionad os dois novos exemplos de contratos de criptografia e alteramos a resolução máxima SD para 1024x576 em todos os exemplos em questão.	27 de janeiro de 2022
Lançamento inicial	Primeira versão do Secure Packager and Encoder Key Exchange (SPEKE) 2.0, uma especificação de comunicaç ão entre um criptografador de conteúdo e um provedor de chaves de DRM. O provedor de chaves DRM expõe uma API Secure Packager and Encoder Key Exchange para	7 de setembro de 2021

Alteração	Descrição	Data
	lidar com as solicitações de chave recebidas.	

AWS Glossário

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.