Spécification d'API Secure Packager and Encoder Key Exchange

Guide des partenaires et clients

Spécification d'API Secure Packager and Encoder Key Exchange: Guide des partenaires et clients

Table of Contents

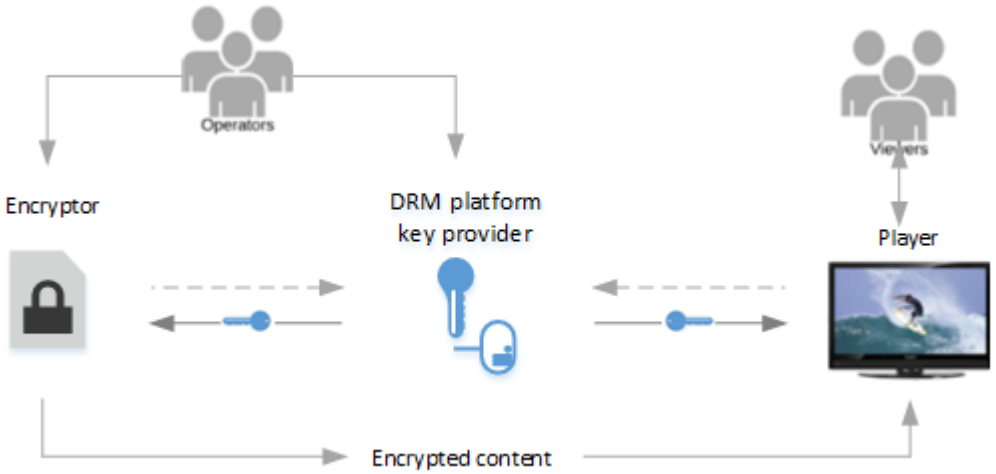
Qu'est-ce que Secure Packager and Encoder Key Exchange ?

Secure Packager and Encoder Key Exchange (SPEKE) définit la norme de communication entre les chiffreurs et les empaqueteurs de contenu multimédia et les fournisseurs de clés de gestion des droits numériques (DRM). La spécification prend en compte les chiffreurs s'exécutant sur site et dans le cloud AWS.

Rubriques

Architecture générale

L'illustration suivante montre une vue générale de l'architecture de chiffrement de contenu SPEKE pour les produits sur site.

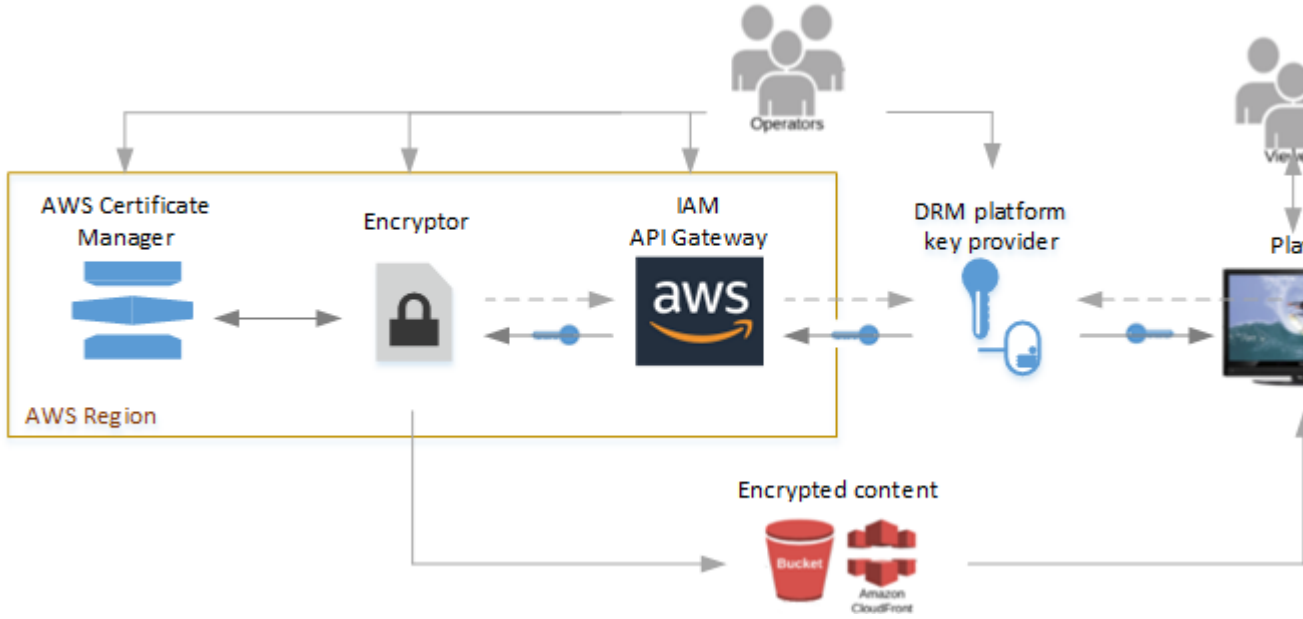


Voici les principaux composants de l'architecture précédente :

- ChiffreurFournit la technologie de chiffrement. Reçoit les demandes de chiffrement de son opérateur et récupère les clés obligatoires à partir du fournisseur de clés DRM pour sécuriser le contenu chiffré.
- Fournisseur de clés de plate-forme DRM— Fournit des clés de chiffrement au chiffreur via une API compatible avec SPEKE. Le fournisseur fournit également des licences aux lecteurs multimédias pour le déchiffrement.
- Joueur— Demande des clés au même fournisseur de clés de la plateforme DRM et les utilise pour déverrouiller le contenu et le mettre à disposition de ses utilisateurs.

Architecture basée sur le cloud AWS

L'illustration suivante montre l'architecture de haut niveau lorsque SPEKE est utilisé avec des services et des fonctions s'exécutant dans le cloud AWS.



Voici les principaux services et composants :

- Chiffreur— Fournit la technologie de chiffrement dans le cloud AWS. Le chiffreur reçoit des demandes de son opérateur et récupère les clés de chiffrement requises auprès du fournisseur de clés DRM, via Amazon API Gateway, pour sécuriser le contenu chiffré. Il transmet le contenu chiffré à un compartiment Amazon S3 ou via Amazon S3 ou via un AmazonCloudFrontdistribution.
- AWS IAM et Amazon API GatewayGèrent les rôles approuvés par le client et la communication proxy entre le chiffreur et le fournisseur de clés. API Gateway fournit des fonctionnalités de journalisation et permet aux clients de contrôler leurs relations avec le chiffreur et avec la plateforme DRM. Les clients activent l'accès au fournisseur de clés via la configuration de rôle IAM. API Gateway doit se trouver dans la même région AWS que le chiffreur.
- AWS Certificate Manager— (Facultatif) Fournit la gestion des certificats pour le chiffrement des clés de contenu. Le chiffrement des clés de contenu est la pratique recommandée pour sécuriser la communication. Le gestionnaire de certificats doit se trouver dans la même région AWS que le chiffreur.
- Fournisseur de clés de plate-forme DRM— Fournit des clés de chiffrement au chiffreur via une API compatible avec SPEKE. Le fournisseur fournit également des licences aux lecteurs multimédias pour le déchiffrement.
- Joueur— Demande des clés au même fournisseur de clés de la plateforme DRM et les utilise pour déverrouiller le contenu et le mettre à disposition de ses utilisateurs.

Comment démarrer

Pour obtenir des informations de base supplémentaires sur SPEKE, veuillez consulterVous débutez avec SPEKE ? (p. 3).

Êtes-vous un client ?

Associez-vous à un fournisseur de plateforme DRM AWS Elemental pour vous préparer à utiliser le chiffrement. Pour plus d'informations, consultez .Intégration de client (p. 5).

Êtes-vous un fournisseur de plateforme DRM ou un client disposant de votre propre fournisseur de clés ?

Utilisez une API REST pour votre fournisseur de clés conformément à la spécification SPEKE. Pour plus d'informations, consultez .Spécification d'API SPEKE (p. 7).

Vous débutez avec SPEKE ?

Cette section fournit des informations de base, pour les lecteurs qui débutent avec Secure Packager et Encoder Key Exchange (SPEKE).

Pour accéder à une présentation de SPEKE, regardez le webcast suivant :

Services et spécifications connexes

- Autorisations API gateway— Contrôle l'accès à une API avec les autorisations AWS Identity and Access Management (AWS IAM).
- AWSAssumeRole— Utilisation d'AWS Security Token Service (AWS STS) pour assumer une fonctionnalité de rôle.
- Sigv4— Signe une demande HTTP à l'aide de Signature Version 4.
- Spécification DASH-IF CPIX v2.0— Version de spécification DASH-IF Content Protection Information Exchange Format (CPIX), sur laquelle se base cette spécification SPEKE v1.0.

- Spécification DASH-IF CPIX v2.3— Version de spécification DASH-IF Content Protection Information Exchange Format (CPIX), sur laquelle se base cette spécification SPEKE v2.0.
- ID système DASH-IF— Liste des identifiants enregistrés pour les systèmes DRM.
- https://github.com/awslabs/speke-reference-server— Exemple de fournisseur de clés de référence à utiliser avec votre compte AWS pour vous aider à démarrer avec une implémentation SPEKE dans AWS.

Terminologie

La liste suivante définit la terminologie utilisée dans cette spécification. Dans la mesure du possible, cette spécification suit la terminologie utilisée dans la spécification DASH-IF CPIX.

- ARN— Amazon Resource Name. Identifie de façon unique une ressource AWS.
- Clé de contenu— Clé cryptographique utilisée pour chiffrer une partie du contenu.
- Fournisseur de contenu— Un éditeur qui fournit les droits et les règles pour fournir des supports protégés. Le fournisseur de contenu peut également fournir un contenu multimédia source (format mezzanine, pour le transcodage), des identifiants de ressource, des identifiants de clé (KID), des valeurs de clé, des instructions d'encodage et des métadonnées de description de contenu.
- GESTION DES DROITS NUMÉRIQUES— Gestion des droits numériques Utilisé pour protéger le contenu numérique protégé par des droits d'auteur contre un accès non autorisé.
- Plateforme DRM— Système qui fournit la fonctionnalité DRM et la prise en charge des chiffreurs de contenu et des utilisateurs, y compris la fourniture de clés DRM et de licences pour le chiffrement et le déchiffrement de contenu.
- Fournisseur DRM— Consultez Plateforme DRM.
- Système DRM— Norme pour les implémentations DRM. Les systèmes DRM courants incluent AppleFairPlay, Google Widevine et MicrosoftPlayReady. Les systèmes DRM sont utilisés par les fournisseurs de contenu pour sécuriser le contenu numérique destiné à être diffusé et accessibles aux utilisateurs. Pour obtenir la liste des systèmes DRM enregistrés auprès de DASH-IF, consultez la pageID système DASH-IF. La spécification DASH-IF CPIX utilise l'expression « système DRM » telle que définie ici et, dans certains cas, elle utilise l'expression « système DRM » pour indiquer à quoi cette spécification fait référence en tant que plateforme DRM.
- Solution DRM— Consultez Plateforme DRM.
- Technologie DRM— Voir Système DRM.
- Chiffreur— Composant de traitement multimédia qui chiffre du contenu multimédia à l'aide de clés obtenues auprès du fournisseur de clés. Les chiffreurs ajoutent généralement également le signalement et les métadonnées de chiffrement DRM au média. Les chiffreurs sont généralement des encodeurs, des empaqueteurs et des transcodeurs.
- Fournisseur de clés— Composant d'une plateforme DRM qui expose une API REST SPEKE afin de gérer les demandes de clés. Le fournisseur de clés peut être le serveur de clés lui-même ou un autre composant de la plateforme.
- Serveur de clés— Composant d'une plateforme DRM qui gère les clés pour le chiffrement et le déchiffrement de contenu.
- "."— Responsable du fonctionnement de l'ensemble du système, y compris du chiffreur et du fournisseur de clés.
- Joueur— Lecteur multimédia exécuté pour le compte d'un utilisateur. Obtient ses informations de différentes sources, notamment les fichiers manifeste multimédias, les fichiers multimédias et les licences DRM. Demande des licences à la plateforme DRM pour le compte des utilisateurs.

Intégration de client

Protégez votre contenu contre une utilisation non autorisée en combinant un fournisseur de clés de système de gestion des droits numériques (DRM) Secure Packager et Encoder Key Exchange (SPEKE) avec votre chiffreur et vos lecteurs multimédias. SPEKE définit la norme de communication entre les chiffreurs et les empaqueteurs de contenu multimédia et les fournisseurs de clés de système de gestion des droits numériques (DRM). Pour commencer l'intégration, vous choisissez un fournisseur de clés de plateforme DRM et configurez la communication entre le fournisseur de clés et vos chiffreurs et lecteurs.

Rubriques

Embalquez avec un fournisseur de plateformes DRM

Les partenaires Amazon suivants fournissent des implémentations de plateformes DRM tierces pour SPEKE. Pour de plus amples informations sur leurs offres et sur la façon de les contacter, suivez les liens vers leurs pages Réseau de partenaires Amazon. Les partenaires qui n'ont pas de lien ne disposent pas actuellement d'une page Réseau de partenaires Amazon, mais vous pouvez les contacter directement. Les partenaires peuvent vous aider à vous préparer à utiliser leurs plateformes.

Fournisseur de plateformes DRM	Prise en charge de SPEKE v1	Prise en charge de SPEKE v2 (AWS Elemental MediaPackage)
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
INKA Entworks	√	√
Insys Video Technologies	√	
Intertrust Technologies	√	√
Irdeto	√	√
Lecteur JW	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	
SeaChange	√	
Verimatrix	√	

Fournisseur de plateformes DRM	Prise en charge de SPEKE v1	Prise en charge de SPEKE v2 (AWS Elemental MediaPackage)
Viaccess-Orca	√	
WebStream	√	

Support SPEKE dans les services et produits AWS

Cette section répertorie le support SPEKE fourni par AWS Media Services qui s'exécute dans le cloud AWS et par les produits multimédias AWS sur site. Ces services et produits sont les chiffreurs de l'architecture de chiffrement de contenu SPEKE. Vérifiez que votre protocole de streaming et le système DRM souhaité sont disponibles pour votre service ou produit.

Service ou produit AWS	Prise en charge de SPEKE v1	Prise en charge de SPEKE v2	Technologies DRM prises en charge
AWS Elemental MediaConvert - Service qui s'exécute dans le cloud AWS	√		Documentation
AWS Elemental MediaPackage - Service qui s'exécute dans le cloud AWS	√	√	Documentation
AWS Elemental Live	√		Documentation : MPEG-DASH/HLS
AWS Elemental Server	√		Documentation

Spécification de l'API SPEKE

Il s'agit de la spécification d'API REST pour Secure Packager and Encoder Key Exchange (SPEKE). Utilisez cette spécification pour fournir une protection des droits d'auteur DRM aux clients qui utilisent le chiffrement.

Dans un flux de travail de streaming vidéo, le moteur de chiffrement communique avec la plateforme DRM pour demander des clés de contenu. Ces clés étant extrêmement sensibles, il est essentiel que le fournisseur de clés et le moteur de chiffrement établissent un canal de communication fiable et hautement sécurisé. Vous pouvez également chiffrer les clés de contenu dans le document pour augmenter la sécurité, end-to-end chiffrement.

Cette spécification répond aux objectifs suivants :

- Définir une interface simple, fiable et hautement sécurisée que les fournisseurs DRM et les clients peuvent utiliser pour l'intégrer à des chiffreurs lorsqu'un chiffrement de contenu est requis.
- Traiter les flux de travail de vidéo à la demande (VOD) et en direct, et inclure les conditions d'erreur et les mécanismes d'authentification qui sont requis pour établir une communication solide et hautement sécurisée entre les chiffreurs et les points de terminaison de fournisseur de clés DRM.
- Inclure la prise en charge des formats d'emballage HLS, MSS et DASH et de leurs systèmes DRM courants : FairPlay, PlayReady et Widevine/CENC.
- Préserver la simplicité et l'extensibilité de la spécification, pour prendre en charge les futurs systèmes DRM.
- Utiliser une API REST simple.

Note

Rubriques

Authentification

SPEKE nécessite une authentification pour les produits sur site, ainsi que pour les services et les fonctions qui s'exécutent dans le cloud AWS.

Rubriques

Authentification pour les implémentations dans le cloud AWS

SPEKE nécessite une authentification AWS via des rôles IAM en vue d'une utilisation avec un chiffreur. Les rôles IAM sont créés par le fournisseur DRM ou par l'opérateur qui possède le point de terminaison DRM dans un compte AWS. Chaque rôle se voit attribuer un Amazon Resource Name (ARN), que l'opérateur de service AWS Elemental fournit sur la console de service lorsque vous demandez le chiffrement. Les autorisations de stratégie du rôle doivent être configurées pour accorder l'autorisation d'accéder à l'API du fournisseur de clés, mais à aucune autre ressource AWS. Lorsque le chiffreur contacte le fournisseur de clés DRM, il utilise l'ARN de rôle pour assumer le rôle du titulaire du compte du fournisseur de clés, qui renvoie des informations d'identification temporaires que le chiffreur utilisera pour accéder au fournisseur de clés.

Généralement, l'opérateur ou le fournisseur de la plateforme DRM utilise Amazon API Gateway devant le fournisseur de clés, puis active l'autorisation AWS Identity and Access Management (AWS IAM) sur la ressource API Gateway. Vous pouvez utiliser l'exemple de définition de stratégie suivant et l'attacher à un nouveau rôle pour accorder des autorisations à la ressource appropriée. Dans ce cas, les autorisations concernent toutes les ressources API Gateway :

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

Enfin, le rôle nécessite l'ajout d'une relation d'approbation et l'opérateur doit être en mesure de sélectionner le service.

L'exemple suivant illustre un ARN de rôle qui est créé pour accéder au fournisseur de clés DRM :

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

Pour plus d'informations sur la création d'un rôle, consultez AWS AssumeRole. Pour plus d'informations sur la signature d'une demande, consultez AWS Sigv4.

Authentification pour les produits sur site

Pour les produits sur site, nous vous recommandons d'utiliser SSL/TLS et l'authentification de la valeur de hachage afin d'atteindre une sécurité optimale. Mais au minimum, vous devez utiliser l'authentification de base sur HTTPS.

Les deux types d'authentification utilisent l'en-tête `Authorization` dans la requête HTTP :

- Authentification résumée— L'en-tête d'autorisation est composé de l'identifiant`Digest`suivi d'une série de valeurs qui authentifient la requête. Plus précisément, une valeur de réponse est générée par le biais d'une série de fonctions de hachage MD5 qui incluent une valeur de réponse unique, one-time-use nonce depuis le serveur utilisé pour garantir que le mot de passe se déplace en toute sécurité.
- L'authentification de base— L'en-tête d'autorisation est composé de l'identifiant`Basic`suivie d'une chaîne codée en Base64 qui représente le nom d'utilisateur et le mot de passe séparés par un signe deux-points.

Pour plus d'informations sur l'authentification de base et de la valeur de hachage, notamment des informations détaillées sur l'en-tête, consultez la spécification Internet Engineering Task Force (IETF).RFC 2617 - Authentification HTTP : Authentification des accès de base et de synthèse.

SPEKE API v1

Pour être conforme à Speke, votre fournisseur de clés DRM doit exposer l'API REST décrite dans cette spécification. Le chiffreur effectue des appels d'API vers votre fournisseur de clés.

> Note
>
> Les exemples de code présentés dans cette spécification sont fournis à des fins d'illustration uniquement. Vous ne pouvez pas exécuter les exemples, car ils ne font pas partie d'une implémentation SPEKE complète.

Secure Packager and Encoder Key Exchange utilise la définition de structure de données DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) pour l'échange de clés, avec certaines restrictions. DASH-IF-CPIX définit un schéma qui permet d'échanger de façon extensible des modèles de gestion des droits numériques entre la plateforme DRM et le chiffreur. Ainsi, le chiffrement de contenu est possible pour tous les formats d'emballage en vitesse de transmission adaptative au moment de la compression et de l'emballage du contenu. Les formats d'emballage en vitesse de transmission adaptative sont les suivants : HLS, DASH et MSS.

Pour plus d'informations sur le format d'échange, consultez la spécification DASH Industry Forum CPIX à l'adresse.https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf.

Rubriques

API SPEKE v1 - Personnalisations et contraintes pour la spécification DASH-IF

La spécification DASH-IF CPIX,https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf, prend en charge un certain nombre de cas d'utilisation et de topologies. La spécification d'API SPEKE est conforme à la spécification CPIX avec les personnalisations et contraintes suivantes :

- SPEKE suit le flux de travail Encryptor Consumer.

- Pour les clés de contenu chiffrées, SPEKE applique les restrictions suivantes :
  - SPEKE ne prend pas en charge la vérification des signatures numériques (XMLDSIG) pour les charges utiles de demandes ou de réponses.
  - SPEKE nécessite 2048 certificats RSA.
- Pour faire pivoter les flux de travail clés, SPEKE requiert l'option`ContentKeyUsageRule`filtre,`KeyPeriodFilter`. SPEKE ignore tous les autres`ContentKeyUsageRule`Paramètres de .
- SPEKE omet la`UpdateHistoryItemList`fonctionnalité. Si la liste est présente dans la réponse, SPEKE l'ignore.
- SPEKE prend en charge la rotation des clés. SPEKE utilise uniquement le `ContentKeyPeriod @index pour suivre la période de clé.
- Pour prendre en charge MSS PlayReady, SPEKE utilise un paramètre personnalisé sous le`DRMSystem`étiquette,`SPEKE:ProtectionHeader`.
- Pour l'emballage HLS, si `URIExtXKey` est présent dans la réponse, il doit contenir toutes les données à ajouter dans le paramètre URI de la balise `EXT-X-KEY` d'une liste de lecture HLS, sans aucune autre exigence de signalement.
- Pour la liste de lecture HLS, sous le`DRMSystem`, SPEKE fournit les paramètres personnalisés optionnels`speke:KeyFormat`et`speke:KeyFormatVersions`, pour les valeurs de la`KEYFORMAT`et`KEYFORMATVERSIONS`paramètres de la`EXT-X-KEY`étiquette.

  Le vecteur d'initialisation (IV) HLS suit toujours le numéro de segment, sauf s'il est explicitement spécifié par l'opérateur.
- Lors de la demande de clés, le chiffreur peut utiliser l'attribut facultatif `@explicitIV` sur l'élément `ContentKey`. Le fournisseur de clés peut répondre avec un vecteur d'initialisation à l'aide de `@explicitIV`, même si l'attribut n'est pas inclus dans la requête.
- Le chiffreur crée l'identifiant de clé (`KID`), qui reste le même quels que soient l'ID de contenu et la durée d'utilisation des clés. Le fournisseur de clés inclut `KID` dans sa réponse au document de demande.
- Le fournisseur de clés peut contenir une valeur pour l'en-tête de réponse `Speke-User-Agent`, qui lui permet de s'identifier à des fins de débogage.
- Actuellement, SPEKE ne prend pas en charge plusieurs pistes ou clés par contenu.

  Le chiffreur conforme à Speke agit en tant que client et envoie`POST`opérations vers le point de terminaison du fournisseur de clés. Le chiffreur peut envoyer une requête `heartbeat` périodique afin de s'assurer que la connexion entre le chiffreur et le point de terminaison du fournisseur de clés est saine.

API SPEKE v1 - Composants de charge utile standard

Dans n'importe quelle requête SPEKE, le chiffreur peut demander des réponses pour un ou plusieurs systèmes DRM. Le chiffreur spécifie les systèmes DRM dans `<cpix:DRMSystemList>` de la charge utile de la demande. Chaque spécification système inclut la clé et indique le type de réponse à renvoyer.

L'exemple suivant présente une liste de système DRM avec une seule spécification de système DRM :

```
<cpix:DRMSystemList>
    <!--I 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>
```

Le tableau suivant répertorie les principaux composants de chaque élément `<cpix:DRMSystem>`.

Identifiant	Description
`systemId` ou `schemeId`	Identifiant unique pour le type de système DRM, tel qu'il est enregistré auprès de l'organisation DASH IF. Pour obtenir une liste, consultez DASH-IF System IDs (ID système DASH-IF).
`kid`	ID de la clé . Il ne s'agit pas de la clé réelle, mais d'un identifiant qui pointe vers la clé dans une table de hachage.
`<cpix:UriExtXKey>`	Demande une clé non chiffrée standard. Le type de réponse de clé doit être celui-ci ou la réponse `PSSH`.
`<cpix:PSSH>`	Demande un en-tête spécifique au système de protection (Protection System Specific Header ou PSSH). Ce type d'en-tête contient une référence à l'élément `kid`, à l'élément `systemID`, ainsi que des données personnalisées pour le fournisseur DRM, dans le cadre du chiffrement commun Common Encryption (CENC). Le type de réponse de clé doit être celui-ci ou la réponse `UriExtXKey`.

_Exemples de demandes pour une clé standard et pour PSSH _

L'exemple suivante affiche un exemple de demande envoyée par le chiffreur au fournisseur de clés DRM. Les principaux composants sont mis en évidence. La première demande concerne une clé standard, tandis que la deuxième concerne une réponse PSSH :

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

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

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

System Id

request Key

System Id

request PSSH

_Exemples de réponses pour une clé standard et pour PSSH _

L'exemple suivante affiche la réponse correspondante envoyée par le fournisseur de clés DRM au chiffreur :

```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix" xmlns:pskc="urn:ietf:params:x
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:Plain
                </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">  <-- System Id

            <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVz
            uY29tL0VrZVN0YWdlL2NsaWVudC9hYmMxMjMvOThlZTU1OTYtY2QzZS1hMjBk
            m</cpix:URIExtXKey>
            <speke:KeyFormat>aWRlbnRpdHk=</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">  <-- System Id

            <cpix:PSSH>AAAAanBzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAAEoIARIQe
            2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOYmI3RGppNnNBdEtaelE9PS
        </cpix:DRMSystem>

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

SPEKE API v1 - Exemples d'appels de méthode de flux de travail en direct

Exemple de syntaxe de la requête

L'URL suivante est un exemple et n'indique pas de format fixe :

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

Corps de la demande

Elément CPIX.

En-têtes de requête

Nom	Type	Se produit	Description
`AWS Authorization`	Chaîne	1..1	Consultez AWS Sigv4
`X-Amz-Security-Token`	Chaîne	1..1	Consultez AWS Sigv4
`X-Amz-Date`	Chaîne	1..1	Consultez AWS Sigv4
`Content-Type`	Chaîne	1..1	application/xml

En-têtes de réponse

Nom	Type	Se produit	Description
`Speke-User-Agent`	Chaîne	1..1	Chaîne qui identifie le fournisseur de clés
`Content-Type`	Chaîne	1..1	application/xml

Réponse à la requête

CODE HTTP	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	Réponse à la charge utile DASH-CPIX
`4XX (Client error)`	Message d'erreur client	1..1	Description de l'erreur client
`5XX (Server error)`	Message d'erreur serveur	1..1	Description de l'erreur serveur

> **Note**
>
> Les exemples de cette section n'incluent pas le chiffrement de clé de contenu. Pour obtenir plus d'informations sur l'ajout de chiffrement de clé de contenu, consultezChiffrement de contenu (p. 19).

Exemple de charge utile de requête en direct avec des clés

L'exemple suivant montre une charge utile de requête en direct standard du chiffreur vers le fournisseur de clés 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>
```

Exemple de charge utile de réponse en direct avec des clés

L'exemple suivant affiche une charge utile de réponse standard provenant du fournisseur de clés 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>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZVN0YWdlI
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>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZVN0YWdlL
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
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOYmI3RGppN
cpix:PSSH>
  </cpix:DRMSystem>

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

 <speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAiAGgAdAB0AHAAOgAvAC
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEkARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQBMAFkAMA
+AGgAdAB0AHAAOgAvAC8AcABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgBlAGMAdAB0AGEAcABzAC4AbgBlAHQALwBwAHIALwBzAHYAYw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

 <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4IhflQAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgAgAHgAbQB
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQQBMAEcASQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPgA8AEMASA
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAcABzADoALw
+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 - Exemples d'appels de méthode de flux de travail VOD

Exemple de syntaxe de la requête

L'URL suivante est un exemple et n'indique pas de format fixe.

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

Corps de la demande

Elément CPIX.

En-têtes de réponse

Nom	Type	Se produit	Description
`Speke-User-Agent`	Chaîne	1..1	Chaîne qui identifie le fournisseur de clés
`Content-Type`	Chaîne	1..1	application/xml

Réponse à la requête

CODE HTTP	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	Réponse à la charge utile DASH-CPIX
`4XX (Client error)`	Message d'erreur client	1..1	Description de l'erreur client
`5XX (Server error)`	Message d'erreur serveur	1..1	Description de l'erreur serveur

> **Note**
>
> Les exemples de cette section n'incluent pas le chiffrement de clé de contenu. Pour obtenir plus d'informations sur l'ajout de chiffrement de clé de contenu, consultezChiffrement de contenu (p. 19).

Exemple de charge utile de requête VOD avec des clés

L'exemple suivant montre une charge utile de requête VOD basique du chiffreur vers le fournisseur de clés 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>
```

Exemple de charge utile de réponse VOD avec des clés

L'exemple suivant affiche une charge utile de réponse VOD basique provenant du fournisseur de clés 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>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZVN0YWdlI
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>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXdlc3QtMi5hbWF6b25hd3MuY29tL0VrZVN0YWdlI
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
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOYmI3RGppN
cpix:PSSH>
  </cpix:DRMSystem>

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

 <speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAiAGgAdAB0AHAAOgAvAC
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEkARAA
```

```
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQBMAFkAMA
+AGgAdAB0AHAAOgAvAC8AcABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgBlAGMAdAB0AGEAcABzAC4AbgBlAHQALwBwAHIALwBzAHYAYw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

 <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4IhflQAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUgAgAHgAbQB
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQQBMAEcASQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPgA8AEMASA
+AGEAVABtAFAASgBWAEMAVgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAcABzADoALw
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
</cpix:CPIX>
```

API SPEKE v1 - Cryptage des clés de contenu

Si vous le souhaitez, vous pouvez ajouter le chiffrement de clé de contenu à votre implémentation SPEKE. Le chiffrement de la clé de contenu garantit end-to-end en chiffrant les clés de contenu en transit, en plus de chiffrer le contenu lui-même. Si vous n'implémentez pas cette fonctionnalité pour votre fournisseur de clés, vous comptez sur le chiffrement de la couche de transport plus sur une authentification solide pour assurer la sécurité.

Pour utiliser le chiffrement de clé de contenu pour les chiffreurs qui s'exécutent dans le cloud AWS, les clients importent des certificats dans AWS Certificate Manager, puis utilisent les ARN de certificat générés pour leurs activités de chiffrement. Le chiffreur utilise les ARN de certificat et le service ACM pour fournir des clés de contenu chiffrées au fournisseur de clés DRM.

Restrictions

SPEKE prend en charge le chiffrement de clé de contenu, comme indiqué dans la spécification DASH-IF CPIX, avec les restrictions suivantes :

- SPEKE ne prend pas en charge la vérification des signatures numériques (XMLDSIG) pour les charges utiles de demandes ou de réponses.
- SPEKE nécessite 2048 certificats RSA.

Ces restrictions sont également répertoriées dansPersonnalisations et contraintes pour la spécification DASH-IF (p. 9).

Implémentation du chiffrement de clé de contenu

Pour fournir un chiffrement de clé de contenu, incluez les éléments suivants dans vos implémentations de fournisseur de clés DRM :

- Traitez l'élément `<cpix:DeliveryDataList>` dans les charges utiles de demande et de réponse.
- Fournissez des valeurs chiffrées dans l'élément `<cpix:ContentKeyList>` des charges utiles de réponse.

Pour de plus amples informations sur ces éléments, veuillez consulter la spécification DASH-IF CPIX 2.0.

Exemple d'élément de chiffrement de clé de contenu `<cpix:DeliveryDataList>` dans la charge utile de requête

L'exemple suivant met en évidence l'élément `<cpix:DeliveryDataList>` ajouté en gras :

```
<?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>
```

Exemple d'élément de chiffrement de clé de contenu `<cpix:DeliveryDataList>` dans la charge utile de réponse

L'exemple suivant met en évidence l'élément `<cpix:DeliveryDataList>` ajouté en gras :

```
<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>
```

Exemple d'élément de chiffrement de clé de contenu `<cpix:ContentKeyList>` dans la charge utile de réponse

L'exemple suivant illustre le traitement de la clé de contenu chiffrée dans l'élément `<cpix:ContentKeyList>` de la charge utile de réponse. Elle utilise l'élément `<pskc:EncryptedValue>` :

```
   <cpix:ContentKeyList>
        <cpix:ContentKey kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
            <cpix:Data>
                <pskc:Secret>
                    <pskc:EncryptedValue>
                        <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
                        <enc:CipherData>
                            <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
                        </enc:CipherData>
                    </pskc:EncryptedValue>
                    <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
                </pskc:Secret>
            </cpix:Data>
        </cpix:ContentKey>
    </cpix:ContentKeyList>
```

En comparaison, l'exemple suivant affiche une charge utile de réponse similaire avec la clé de contenu non chiffrée, comme une clé en clair. Elle utilise l'élément `<pskc:PlainValue>` :

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

API SPEKE v1 - Heartbeat

Exemple de syntaxe de la requête

L'URL suivante est un exemple et n'indique pas de format fixe :

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

Réponse à la requête

CODE HTTP	Nom de la charge utile	Se produit	Description
`200 (Success)`	statusMessage	1..1	Message décrivant le statut

API SPEKE v1 - Remplacer l'identificateur de clé

Le chiffreur crée un nouvel identifiant de clé (KID) chaque fois qu'il effectue une rotation des clés. Il transmet le KID au fournisseur de clés DRM dans ses demandes. Le fournisseur de clés répond presque toujours à l'aide du même KID, mais il peut fournir une autre valeur pour le KID dans la réponse.

Voici un exemple de demande avec le KID `11111111-1111-1111-1111-111111111111` :

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

La réponse suivante remplace le KID par `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
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOYmI3RGppN
cpix:PSSH>
      </cpix:DRMSystem>
     </cpix:DRMSystemList>
     <cpix:ContentKeyPeriodList>
      <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
     </cpix:ContentKeyPeriodList>
     <cpix:ContentKeyUsageRuleList>
      <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222">
       <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
      </cpix:ContentKeyUsageRule>
     </cpix:ContentKeyUsageRuleList>
```

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

SPEKE API v2

Pour être conforme à Speke, votre fournisseur de clés DRM doit exposer l'API REST décrite dans cette spécification. Le chiffreur effectue des appels d'API vers votre fournisseur de clés.

> Note
>
> Les exemples de code présentés dans cette spécification sont fournis à des fins d'illustration uniquement. Vous ne pouvez pas exécuter les exemples, car ils ne font pas partie d'une implémentation SPEKE complète.

Secure Packager and Encoder Key Exchange utilise la définition de structure de données DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) pour l'échange de clés, avec certaines restrictions. DASH-IF-CPIX définit un schéma qui permet d'échanger de façon extensible des modèles de gestion des droits numériques entre la plateforme DRM et le chiffreur. Ainsi, le chiffrement de contenu est possible pour tous les formats d'emballage en vitesse de transmission adaptative au moment de la compression et de l'emballage du contenu. Les formats d'emballage en vitesse de transmission adaptative sont les suivants : HLS, DASH et MSS.

À partir de sa version 2.0, SPEKE est aligné sur une version CPIX spécifique :

Du côté de SPEKE, cela est appliqué grâce à l'utilisation du`X-Speke-Version`En-tête HTTP, et du côté CPIX via l'utilisation du`CPIX@version`Attribut. L'absence de ces éléments dans les requêtes est typique des flux de travail hérités de SPEKE v1. Dans les workflows SPEKE v2, le fournisseur de clés ne doit traiter les documents CPIX que s'il prend en charge les deux paramètres de version.

Pour obtenir plus d'informations sur le format d'échange, consultez le DASH Industry ForumSpécification CPIX 2.3.

Dans l'ensemble, SPEKE v2.0 apporte les évolutions suivantes par rapport à SPEKE v1.0 :

- Toutes les balises de l'espace de noms XML SPEKE sont déconseillées au profit des balises équivalentes dans l'espace de noms XML CPIX
- `SPEKE:ProtectionHeader`est obsolète et remplacé par`CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`,`SPEKE:KeyFormat`et`SPEKE:KeyFormatVersions`sont obsolètes et remplacés par`CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id`est remplacé par`CPIX@contentId`
- Nouveaux attributs CPIX obligatoires :`CPIX@version`,`ContentKey@commonEncryptionScheme`
- Nouvel élément CPIX en option :`DRMSystem.ContentProtectionData`
- Support de plusieurs clés de contenu
- Mécanisme de versionnement croisé entre SPEKE et CPIX
- Evolution des en-têtes HTTP : nouveau`X-Speke-Version`Header,`Speke-User-Agent`En-tête renommé en`X-Speke-User-Agent`
- Dépréciation de l'API de pulsation

Comme la spécification SPEKE v1.0 reste inchangée, les implémentations existantes n'ont pas besoin de changer pour continuer à prendre en charge les flux de travail SPEKE v1.0.

Rubriques

- Speke API v2 - Personnalisations et contraintes pour la spécification DASH-IF (p. 24)
- API SPEKE v2 - Composants de charge utile standard (p. 26)

Speke API v2 - Personnalisations et contraintes pour la spécification DASH-IF

Le Forum de l'industrie DASHSpécification CPIX 2.3prend en charge un certain nombre de cas d'utilisation et de topologies. La spécification SPEKE API v2.0 définit à la fois un profil CPIX et une API pour CPIX. Pour atteindre ces deux objectifs, il est conforme à la spécification CPIX avec les personnalisations et contraintes suivantes :

Profil CPIX

- SPEKE suit le flux de travail Encryptor Consumer.
- Pour les clés de contenu chiffrées, SPEKE applique les restrictions suivantes :
  - SPEKE ne prend pas en charge la vérification des signatures numériques (XMLDSIG) pour les charges utiles de demandes ou de réponses.
  - SPEKE nécessite 2048 certificats RSA.
- SPEKE exploite uniquement un sous-ensemble de fonctionnalités CPIX :
  - SPEKE omet la`UpdateHistoryItemList`fonctionnalité. Si la liste est présente dans la réponse, SPEKE l'ignore.
  - SPEKE omet la fonctionnalité de touche racine/feuille. Si l'icône`ContentKey@dependsOnKey`est présent dans la réponse, SPEKE l'ignore.
  - SPEKE omet la`BitrateFilter`Élément et`VideoFilter@wcg`Attribut. Si ces éléments ou attributs sont présents dans la charge utile CPIX, SPEKE l'ignore.
- Seuls les éléments ou attributs référencés comme étant « pris en charge » sur lePage Composants de charge utile standard (p. 26)ou lePage du contrat de chiffrement (p. 29)peut être utilisé dans les documents CPIX échangés avec SPEKE v2.
- Lorsqu'ils sont inclus dans une demande CPIX par le chiffreur, tous les éléments et attributs doivent porter une valeur valide dans la réponse CPIX du fournisseur de clés. Si ce n'est pas le cas, le chiffreur doit s'arrêter et déclencher une erreur.
- SPEKE prend en charge la rotation des clés avec`KeyPeriodFilter`éléments. SPEKE utilise uniquement le`ContentKeyPeriod@index`pour suivre la durée d'utilisation des clés.
- Pour la signalisation HLS, plusieurs`DRMSystem.HLSSignalingData`les éléments doivent être utilisés : un avec un`DRMSystem.HLSSignalingData@playlist`valeur attributaire de « media », et un autre avec un`DRMSystem.HLSSignalingData@playlist`valeur attributaire de « maître ».
- Lors de la demande de clés, le chiffreur peut utiliser l'attribut facultatif `@explicitIV` sur l'élément `ContentKey`. Le fournisseur de clés peut répondre avec un vecteur d'initialisation à l'aide de `@explicitIV`, même si l'attribut n'est pas inclus dans la requête.
- Le chiffreur crée l'identifiant de clé (`KID`), qui reste le même quels que soient l'ID de contenu et la durée d'utilisation des clés. Le fournisseur de clés inclut `KID` dans sa réponse au document de demande.
- Le chiffreur doit inclure une valeur pour le`CPIX@contentId`Attribut. Lorsque vous recevez une valeur vide pour cet attribut, le fournisseur de clés doit renvoyer une erreur avec la description « CPIX @contentId manquant ».`CPIX@contentId`La valeur ne peut pas être remplacée par le fournisseur de clés.

  `CPIX@id`valeur, si elle n'est pas nulle, doit être ignorée par le fournisseur de clés.

- Le chiffreur doit inclure une valeur pour le`CPIX@version`Attribut. Lorsque vous recevez une valeur vide pour cet attribut, le fournisseur de clés doit renvoyer une erreur avec la description « CPIX @version manquant ». Lorsque vous recevez une demande avec une version non prise en charge, la description de l'erreur renvoyée par le fournisseur de clés doit être « CPIX @version non pris en charge ».

  `CPIX@version`La valeur ne peut pas être remplacée par le fournisseur de clés.
- Le chiffreur doit inclure une valeur pour le`ContentKey@commonEncryptionScheme`pour chaque clé demandée. Lorsque vous recevez une valeur vide pour cet attribut, le fournisseur de clés doit renvoyer une erreur avec la description 'Missing ContentKey @commonEncryptionScheme for KID`id` ».

  Un document CPIX unique ne peut pas mélanger plusieurs valeurs pour différentes valeurs`ContentKey@commonEncryptionScheme`Attributs. Lors de la réception d'une telle combinaison, le fournisseur de clés doit renvoyer une erreur avec la description « Combinaison ContentKey @commonEncryptionScheme non conforme ».

  Pas tous`ContentKey@commonEncryptionScheme`les valeurs sont compatibles avec toutes les technologies DRM. Lors de la réception d'une telle combinaison, le fournisseur de clés doit renvoyer une erreur avec la description « ContentKey @commonEncryptionScheme non compatible avec DRMSystem »`id` ».

  `ContentKey@commonEncryptionScheme`La valeur ne peut pas être remplacée par le fournisseur de clés.
- Lorsque vous recevez des valeurs différentes pour`DRMSystem@PSSH`et`DRMSystem.ContentProtectionData`XML interne`<pssh>`dans le corps de réponse CPIX, le chiffreur doit arrêter et déclencher une erreur.

API pour CPIX

- Le fournisseur de clés doit inclure une valeur pour le`X-Speke-User-Agent`En-tête de réponse HTTP.
- Un chiffreur conforme à Speke agit en tant que client et envoie les opérations POST au point de terminaison du fournisseur de clés.
- Le chiffreur doit inclure une valeur pour le`X-Speke-Version`En-tête de requête HTTP, avec la version SPEKE utilisée avec la requête, formulé comme MajorVersion.MinorVersion, comme '2.0' pour SPEKE v2.0. Si le fournisseur de clés ne prend pas en charge la version SPEKE utilisée par le chiffreur pour la demande en cours, le fournisseur de clés doit renvoyer une erreur avec la description « Version SPEKE non prise en charge » et ne doit pas essayer de traiter le document CPIX de manière optimale.

  Le`X-Speke-Version`la valeur d'en-tête définie par le chiffreur ne peut pas être modifiée par le fournisseur de clés dans la réponse à la demande.
- Lors de la réception d'erreurs dans le corps de réponse, le chiffreur doit générer une erreur et ne pas réessayer la demande avec un versionnement SPEKE v1.0.

  Si le fournisseur de clés ne renvoie pas d'erreur mais ne parvient pas à renvoyer un document CPIX contenant les informations obligatoires, le chiffreur doit arrêter et lancer une erreur.

Le tableau suivant résume les messages standard qui doivent être renvoyés par le fournisseur de clés dans le corps du message. Dans les cas d'erreur, le code de réponse HTTP doit être un 4XX ou un 5XX, jamais un 200. Le code d'erreur 422 peut être utilisé pour toutes les erreurs liées à SPEKE/CPIX.

Cas d'erreur	Error message (Message d'erreur)
CPIX @contentId n'est pas défini	CPIX manquant @contentId
CPIX @version n'est pas défini	CPIX manquant @version

Cas d'erreur	Error message (Message d'erreur)
CPIX @version n'est pas pris en charge	CPIX @version non pris en charge
ContentKey @commonEncryptionScheme n'est pas défini	ContentKey @commonEncryptionScheme manquant pour KIDid(oùidest égal à la valeur ContentKey @kid)
Plusieurs valeurs ContentKey @commonEncryptionScheme utilisées dans un seul document CPIX	Combinaison ContentKey @commonEncryptionScheme non conforme
ContentKey @commonEncryptionScheme n'est pas compatible avec la technologie DRM	ContentKey @commonEncryptionScheme non compatible avec DRMSystemid(oùidest égal à DRMSystem @systemId (valeur)
La valeur d'en-tête X-Speke-Version n'est pas une version SPEKE prise en charge	Version SPEKE non prise en charge
Le contrat de chiffrement est mal formé	Contrat de chiffrement mal formé
Le contrat de chiffrement contredit les contraintes liées aux niveaux de sécurité DRM	Contrat de chiffrement CPIX demandé non pris en charge
Le contrat de chiffrement n'inclut pas VideoFilter ou AudioFilter élément	Contrat de chiffrement CPIX manquant

API SPEKE v2 - Composants de charge utile standard

Par le biais d'une seule demande SPEKE, le chiffreur peut demander plusieurs clés de contenu, ainsi que la signalisation manifeste nécessaire pour plusieurs formats d'emballage, conformément au contrat de chiffrement défini pour un contenu donné.

Afin de couvrir tous ces aspects, un document CPIX standard est composé de trois sections de liste obligatoires, ainsi qu'une section de liste facultative pour la rotation des clés de contenu en direct.

<cpix:ContentKeyList><cpix:CPIX>élément de section et de niveau supérieur

Il s'agit d'une section obligatoire, pertinente pour le streaming en direct et en VOD, définissant les différentes clés de contenu devant être utilisées par le chiffreur. Le`<cpix:ContentKeyList>`peut contenir un ou plusieurs éléments`<cpix:ContentKey>`éléments enfants, chacun décrivant une clé de contenu distincte.

Conformément à la spécification CPIX, les valeurs possibles du`ContentKey@commonEncryptionScheme`sont définis dans la spécification Chiffrement commun dans les fichiers de format de fichier de support de base ISO (ISO/IEC 23001-7:2016) :

- « cenc » : Chiffrement complet d'échantillons et de sous-échantillons vidéo en mode AES-CTR
- « cbc1 » : Chiffrement complet d'échantillons et de sous-échantillons vidéo NAL en mode AES-CBC
- « cens » : Chiffrement de modèle NAL vidéo partiel en mode AES-CTR
- « cbcs » : Chiffrement de modèle NAL vidéo partiel en mode AES-CBC

L'exemple suivant montre un document CPIX avec une seule clé de contenu non chiffrée :

```
<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>
```

Par défaut, les clés de contenu ne sont pas chiffrées, comme dans l'exemple ci-dessous. Mais le chiffrement des clés de contenu peut être demandé par le chiffreur via l'inclusion de l'<cpix:DeliveryDataList>élément. Pour en savoir plus, consultez la section Encryption de clé de contenu.

Élément pris en charge par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments enfants obligatoires	Éléments enfants facultatifs
<cpix:CPIX>	ContentID, version, xmlns : cpix, xmlns : pskc	nom, xmlns:enc	un<cpix:ContentKeyList>, un<cpix:DRMSystemList>, un <cpix:ContentKeyUsageRuleList>	un<cpix:DeliveryDataList>, un <cpix:ContentKeyPeriodList>
<cpix:ContentKeyList>		id	au moins un <cpix:ContentKey>	-
<cpix:ContentKey>	enfant, Schéma de chiffrement commun, données	id, algorithme, explicitiv	un <pskc:Secret>	-
<pskc:Secret>	PlainValue ou EncryptedValue	Mac Value	-	<enc:EncryptionMethod>, <enc:CipherData>

<cpix:DRMSystemList>section

Il s'agit d'une section obligatoire, pertinente pour le streaming en direct et la VOD, définissant les différents systèmes DRM qui doivent être exploités avec les clés de contenu.

L'exemple suivant présente une liste de système DRM avec une seule PlayReady Spécification du système 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>
```

Pour obtenir la liste complète des DDRM SystemID, veuillez consulter leSection Protection du contenudu référentiel DASH-IF Identifiers.

Élément pris en charge par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments enfants obligatoires	Éléments enfants facultatifs
<cpix:DRMSystemList>		id	au moins un <cpix:DRMSystem>	-
<cpix:DRMSystem>	enfant, SystemID	ID, nom, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHead deux <cpix:HLSSignalingData>élément avec une valeur d'attribut de liste de lecture différente

`DRMSystem@PSSH`est obligatoire si l'encapsulation ISO-BMFF est appliquée à des segments de support.`DRMSystem.ContentProtectionData`XML interne`<pssh>`est exploité par le chiffreur uniquement à des fins de signalisation manifeste.

Si`DRMSystem@PSSH`est présent et`DRMSystem.ContentProtectionData`contient un InnerXML`<pssh>`, les deux valeurs doivent être identiques.

Si`DRMSystem`la signalisation doit être portée dans les manifestes HLS, à la fois`<cpix:HLSSignalingData playlist="media">`et un`<cpix:HLSSignalingData playlist="master">`les éléments doivent être inclus dans la demande et la réponse CPIX.

<cpix:ContentKeyPeriodList>section

Il s'agit d'une section facultative, pertinente uniquement pour la diffusion en direct, définissant les périodes de chiffrement appliquées au contenu.

Le`<cpix:ContentKeyPeriodList>`peut contenir un ou plusieurs éléments`<cpix:ContentKeyPeriod>`éléments enfants, chacun décrivant une période de chiffrement distincte dans la chronologie en direct. L'utilisation d'UUID comme partie de la valeur de l'attribut id est une approche couramment utilisée.

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

Élément pris en charge par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments enfants obligatoires	Éléments enfants facultatifs
<cpix:ContentKeyPeriodList>		id	au moins un <cpix:ContentKeyPeriod>	-
<cpix:ContentKeyPeriod>	ID, index	-	-	-

Si des périodes de chiffrement sont utilisées, les clés de chiffrement doivent également être attachées à l'une des périodes de chiffrement du document CPIX, comme indiqué dans la section ci-dessous.

<cpix:ContentKeyUsageRuleList>section

Il s'agit d'une section obligatoire, pertinente pour le streaming en direct et en VOD, qui définit comment les différentes clés de contenu protègent les pistes à l'intérieur du streaming et pendant les périodes de chiffrement.

L'<cpix:ContentKeyUsageRuleList>élément peut contenir un ou plusieurs <cpix:ContentKeyUsageRule>éléments enfants, chacun décrivant les pistes auxquelles une clé de contenu donnée est appliquée par le chiffreur, potentiellement pendant une période de chiffrement spécifique. Au moins un <cpix:AudioFilter>ou un <cpix:VideoFilter>élément doit être présent dans un <cpix:ContentKeyUsageRule>élément.

L'exemple suivant montre une liste simple avec une seule règle qui applique une seule clé de contenu à toutes les pistes audio et vidéo pendant une période de chiffrement spécifique.

```
<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>
```

Élément pris en charge par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments enfants obligatoires	Éléments enfants facultatifs
<cpix:ContentKeyUsageRuleList>	-	id	au moins un <cpix:ContentKeyUsageRule>	-
<cpix:ContentKeyUsageRule>	kid, intendedTrackType de piste prévu	-	au moins un <cpix:AudioFilter>ou un <cpix:VideoFilter>(*)	<cpix:KeyPeriodFilter>
<cpix:KeyPeriodFilter>	id PérioD	-	-	-
<cpix:AudioFilter>	-	Chaînes MIN, canaux Max	-	-
<cpix:VideoFilter>	-	MinPixels, MaxPixels, HDR, MinFPS, MaxFPS	-	-

(*) Pour obtenir des explications détaillées sur l'utilisation d'une ou de plusieurs clés de contenu pour protéger une ou plusieurs pistes dans un streaming, veuillez consulter leContrat de cryp (p. 29)section documentation. _

API SPEKE v2 - Contrat de chiffrement

Le contrat de chiffrement définit les clés de contenu qui protègent les pistes à l'intérieur d'un flux donné, en fonction des caractéristiques des pistes.

L'utilisation de plusieurs clés de contenu pour différentes pistes dans un streaming, bien qu'elle soit recommandée dans le secteur, n'est pas obligatoire, mais recommandée : au moins deux touches de contenu différentes, une pour les pistes audio et une pour les pistes vidéo. L'utilisation d'une clé de contenu unique pour chiffrer plusieurs pistes est possible, mais elle doit être explicitement signalée dans le document CPIX envoyé par le chiffreur au fournisseur de clés. De manière générale, le chiffreur décrit toujours avec précision le nombre de clés de contenu nécessaires et la manière dont elles sont exploitées pour chiffrer les différentes pistes multimédia.

Principes

Le contrat de chiffrement se trouve dans le`<cpix:ContentKeyUsageRuleList>`du document CPIX. Dans cette section, chaque clé de contenu définie dans le`<cpix:ContentKeyList>`correspond à une section spécifique`<cpix:ContentKeyUsageRule>`, qui doit comprendre :

- un`ContentKeyUsageRule@intendedTrackType`qui peut référencer un ou plusieurs sous-composants, séparés par le signe « + » si plusieurs sous-composants sont utilisés. Pour`ContentKeyUsageRule@intendedTrackType`doit être unique dans un contrat de chiffrement et ne peut pas être utilisé dans plusieurs`ContentKeyUsageRule`éléments.
- un ou plusieurs`<cpix:AudioFilter>`ou`<cpix:VideoFilter>`élément enfant, en fonction de la valeur de`ContentKeyUsageRule@intendedTrackType`Attribut.

Les règles régissant cette relation sont les suivantes :

- Lorsque toutes les pistes audio et vidéo du streaming doivent être protégées par une clé de contenu unique, la chaîne`'ALL'`doit être utilisé comme`ContentKeyUsageRule@intendedTrackType`valeur d'attribut. L'exemple 1 montre un tel cas d'utilisation. Dans cette situation, les deux`<cpix:AudioFilter />`et un`<cpix:VideoFilter />`les éléments enfants sans attribut doivent être inclus. Toute autre combinaison de`<cpix:AudioFilter>`et/ou`<cpix:VideoFilter>`éléments n'est pas valide dans ce contexte particulier.
- Pour tous les autres cas d'utilisation, la valeur du`ContentKeyUsageRule@intendedTrackType`peut être librement défini et le nombre de`<cpix:AudioFilter />`et un`<cpix:VideoFilter />`les éléments enfants doivent correspondre au nombre de sous-composants agrégés par le signe « + ». Les exemples 2/3/4/5/6/7/9/10 illustrent cette exigence, lorsqu'un seul sous-composant est présent dans le`ContentKeyUsageRule@intendedTrackType`valeur d'attribut. L'exemple 8 illustre le cas où plusieurs sous-composants sont utilisés :`ContentKeyUsageRule@intendedTrackType="SD+HD"`est décrit par deux distincts`<cpix:VideoFilter>`les éléments enfants avec des valeurs d'attributs différentes, et`ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"`est décrit par trois distincts`<cpix:VideoFilter>`éléments enfants avec des valeurs d'attributs différentes.

Filtres

CPIX définit plusieurs éléments et attributs de filtrage, mais SPEKE ne prend en charge qu'un sous-ensemble de celui-ci. Le tableau suivant résume ces différences :

Type de filtre CPIX	Prise en charge globale de SPEKE	Attributs de filtre pris en charge par SPEKE	Attributs de filtre non pris en charge par SPEKE
<cpix:VideoFilter>	Oui	MinPixels, MaxPixels, hdr, MinFPS, MaxFPS (attributs facultatifs)	wcg
<cpix:AudioFilter>	Oui	MinChannels, MaxChannels (attributs facultatifs)	
<cpix:KeyPeriodFilter>	Oui	PerioID (attribut obligatoire)	
<cpix:BitrateFilter>	Non	N/A	N/A
<cpix:LabelFilter>	Non	N/A	N/A

Conformément à la spécification CPIX pour VideoFilter, [MinPixels, MaxPixels] est une plage tout compris dans les deux dimensions, tandis que (MinFPS, MaxFPS] n'est inclusif que pour la dimension MaxFPS. Pour AudioFilter, [MinChannels, MaxChannels] est une plage inclusive dans les deux dimensions.

Situations problématiques

Dans certains cas, les informations fournies dans le contrat de chiffrement peuvent être partielles, ambiguës ou erronées. Dans ces cas, il est important que le chiffreur et le fournisseur de clés se comportent correctement et garantissent une protection adéquate du contenu. Le tableau suivant présente le comportement recommandé dans ces situations :

Dans cette situation	Le chiffreur devrait/doit...	Le fournisseur de clés devrait ou doit...
Aucune règle ne s'applique à une ou plusieurs pistes du streaming (voir l'exemple 3 ci-dessous)	Le chiffreur doit examiner sa configuration (externe à la charge utile CPIX) et vérifier que les pistes concernées ne nécessitent pas de chiffrement. Si ce n'est pas le cas, le chiffreur doit déclencher une erreur et arrêter le traitement.	Non pertinent : le fournisseur de clés ne connaît pas la structure Streamset.
Plusieurs règles se chevauchent et suggèrent plusieurs clés de contenu pour chiffrer une piste spécifique	Le chiffreur doit appliquer le dernier ContentKeyUsageRule évalué avec succès dans l'ordre du document.	Non pertinent : le fournisseur de clés ne connaît pas la structure Streamset.
Le contrat de chiffrement change dans un seul cycle de demande/réponse SPEKE	Le chiffreur doit déclencher une exception et arrêter le traitement, car le fournisseur de clés n'est pas responsable de la définition du contrat de chiffrement.	Pour éviter que cette situation ne se produise en premier lieu, le fournisseur de clés ne doit pas modifier un contrat de chiffrement reçu dans la charge utile CPIX de la demande SPEKE.
Contrat de chiffrement mal formé : exception de contrainte de cardinalité intendedTrackType/Filters, filtres ou attributs non pris en charge	Le chiffreur doit déclencher une exception, arrêter le traitement et ne pas envoyer la demande SPEKE au fournisseur de clés, car cela entraînerait probablement une protection erronée du contenu ou laisserait certaines pistes non protégées.	Le fournisseur de clés doit déclencher une exception et renvoyer une erreur de « contrat de chiffrement mal formé ».
Contrat de chiffrement bien formé, mais en violation des contraintes liées aux niveaux de sécurité DRM : par exemple, une seule clé de contenu est demandée pour protéger les pistes audio et les pistes vidéo UHD	Si le chiffreur a connaissance des contraintes liées aux niveaux de sécurité DRM, il doit déclencher une exception, arrêter le traitement et ne pas envoyer la demande SPEKE au fournisseur de clés, car cela entraînerait probablement une protection erronée du contenu.	Le fournisseur de clés déclenche une exception et renvoie une erreur « Contrat de chiffrement CPIX demandé non pris en charge ».
Contrat de chiffrement absent	Le chiffreur ne doit pas envoyer de documents CPIX qui ne contiennent aucun VideoFilter ou AudioFilter élément.	Le fournisseur de clés doit déclencher une exception et renvoyer une erreur « Contrat de chiffrement CPIX manquant ».

Exemples de contrats de chiffrement

Exemple 1 : une touche de contenu pour toutes les pistes audio et vidéo

```
<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>
```

Exemple 2 : une clé de contenu pour toutes les pistes vidéo, une touche de contenu pour toutes les pistes audio

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

Exemple 3 : une clé de contenu pour toutes les pistes vidéo, pistes audio non chiffrées

```
<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>
```

Exemple 4 : plusieurs touches de contenu pour différentes pistes vidéo (SD/HD), une touche de contenu pour toutes les pistes audio

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD video tracks (more than 1024x576) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
```

```
</cpix:ContentKeyUsageRuleList>
```

Exemple 5 : plusieurs touches de contenu pour différentes pistes vidéo (SD/HD/UHD), une touche de contenu pour toutes les pistes audio

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD video tracks (more than 1920x1080) -->
 <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
 intendedTrackType="UHD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Exemple 6 : plusieurs touches de contenu pour différentes pistes vidéo (SD/HD/UHD1/UHD2), une touche de contenu pour toutes les pistes audio

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
 <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
 intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD2 video tracks (more than 4096x2160) -->
 <cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
 intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
```

```
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Exemple 7 : plusieurs touches de contenu pour différentes pistes vidéo (SD/HD1/HD2/UHD1/UHD2), une touche de contenu pour toutes les pistes audio

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD video tracks (up to 1024x576) -->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HD1 video tracks (more than 1024x576, up to 1280x720) -->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="921600" />
 </cpix:ContentKeyUsageRule>
        <!-- Rule for HD2 video tracks (more than 1280x720, up to 1920x1080) -->
          <cpix:ContentKeyUsageRule kid="cda406d8-9d87-4f76-92da-31110e756176"
 intendedTrackType="HD2">
            <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
            <cpix:VideoFilter minPixels="921601" maxPixels="2073600" />
          </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
 <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
 intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for UHD2 video tracks (more than 4096x2160) -->
 <cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
 intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks -->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Exemple 8 : plusieurs clés de contenu pour différentes pistes vidéo (basées sur plusieurs types d'attributs), une clé de contenu pour toutes les pistes audio

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for SD and HD video tracks-->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff" intendedTrackType="SD
+HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="442368" maxFps="30" hdr="false"/>
  <cpix:VideoFilter minPixels="442369" maxPixels="2073600" maxFps="30" hdr="false"/>
 </cpix:ContentKeyUsageRule>
 <!-- Rule for HDR, HFR and UHD video tracks-->
 <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
 intendedTrackType="HDR+HFR+UHD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
```

```
  <cpix:VideoFilter hdr="true" />
  <cpix:VideoFilter minFps="30" />
  <cpix:VideoFilter minPixels="20736001" />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for all audio tracks-->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
 </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Exemple 9 : une touche de contenu pour toutes les pistes vidéo, plusieurs touches de contenu pour les pistes audio stéréo et 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>
```

Exemple 10 : une touche de contenu pour toutes les pistes vidéo, plusieurs touches de contenu pour la chaîne stéréo et deux types de pistes audio multicanaux

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for video tracks-->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
 </cpix:ContentKeyUsageRule>
 <!-- Rule for stereo audio tracks-->
 <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
 </cpix:ContentKeyUsageRule>
 <!-- Rule for multichannel audio tracks (3 to 6 channels)-->
 <cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
 intendedTrackType="MULTICHANNEL_AUDIO_3_6">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="3" maxChannels="6"/>
 </cpix:ContentKeyUsageRule>
  <!-- Rule for multichannel audio tracks (7 channels and more)-->
 <cpix:ContentKeyUsageRule kid="81eb3761-55ff-4d22-a31d-94f01bbfd8ba"
 intendedTrackType="MULTICHANNEL_AUDIO_7">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="7"/>
```

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

SPEKE API v2 - Exemples d'appels de méthode de flux de travail en direct

Exemple de syntaxe de la requête

L'URL suivante est un exemple et n'indique pas de format fixe :

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

Corps de la demande

Un document CPIX.

En-têtes de requête

Nom	Type	Se produit	Description
`AWS Authorization`	Chaîne	1..1	Consultez AWS Sigv4
`X-Amz-Security-Token`	Chaîne	1..1	Consultez AWS Sigv4
`X-Amz-Date`	Chaîne	1..1	Consultez AWS Sigv4
`Content-Type`	Chaîne	1..1	application/xml
`X-Speke-Version`	Chaîne	1..1	Version de l'API SPEKE utilisée avec la requête, formulée comme MajorVersion.MinorVersion, comme '2.0' pour SPEKE v2.0

En-têtes de réponse

Nom	Type	Se produit	Description
`X-Speke-User-Agent`	Chaîne	1..1	Chaîne qui identifie le fournisseur de clés
`Content-Type`	Chaîne	1..1	application/xml

Réponse à la requête

CODE HTTP	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	Réponse à la charge utile DASH-CPIX

CODE HTTP	Nom de la charge utile	Se produit	Description
`4XX (Client error)`	Message d'erreur client	1..1	Description de l'erreur client
`5XX (Server error)`	Message d'erreur serveur	1..1	Description de l'erreur serveur

> **Note**
>
> Les exemples de cette section n'incluent pas le chiffrement de clé de contenu. Pour obtenir plus d'informations sur l'ajout de chiffrement de clé de contenu, consultezChiffrement de contenu (p. 43).

Exemple de charge utile de requête en direct avec des clés

L'exemple suivant affiche une charge utile de requête en direct standard du chiffreur vers le fournisseur de clés DRM, avec une clé de contenu pour toutes les pistes vidéo et une clé de contenu pour toutes les pistes audio :

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="94ce86fb-07ff-4f43-
adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="94ce86fb-07ff-4f43-
adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="9a04f079-9840-4286-
ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
```

```
   <cpix:SmoothStreamingProtectionHeaderData></cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="9a04f079-9840-4286-
ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Exemple de charge utile de réponse en direct avec des clés

L'exemple suivant affiche une charge utile de réponse classique provenant du fournisseur de clés DRM (les valeurs renvoyées ont été raccourcies par [...] pour plus de précision) :

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

```
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
   <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">lTznjvtzL[...]GfJ</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
   <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
  </cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="9a04f079-9840-4286-
ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
   <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="9a04f079-9840-4286-
ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
   <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2 - Exemples d'appels de méthode de flux de travail VOD

Exemple de syntaxe de la requête

L'URL suivante est un exemple et n'indique pas de format fixe.

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

Corps de la demande

Un document CPIX.

En-têtes de requête

Nom	Type	Se produit	Description
`AWS Authorization`	Chaîne	1..1	Consultez AWS Sigv4
`X-Amz-Security-Token`	Chaîne	1..1	Consultez AWS Sigv4
`X-Amz-Date`	Chaîne	1..1	Consultez AWS Sigv4
`Content-Type`	Chaîne	1..1	application/xml
`X-Speke-Version`	Chaîne	1..1	Version de l'API SPEKE utilisée avec la requête, formulée comme MajorVersion.MinorVersion, comme '2.0' pour SPEKE v2.0

En-têtes de réponse

Nom	Type	Se produit	Description
`X-Speke-User-Agent`	Chaîne	1..1	Chaîne qui identifie le fournisseur de clés
`Content-Type`	Chaîne	1..1	application/xml

Réponse à la requête

CODE HTTP	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	Réponse à la charge utile DASH-CPIX
`4XX (Client error)`	Message d'erreur client	1..1	Description de l'erreur client
`5XX (Server error)`	Message d'erreur serveur	1..1	Description de l'erreur serveur

> **Note**
>
> Les exemples de cette section n'incluent pas le chiffrement de clé de contenu. Pour obtenir plus d'informations sur l'ajout de chiffrement de clé de contenu, consultezChiffrement de contenu (p. 43).

Exemple de charge utile de requête VOD avec des clés

L'exemple suivant affiche une charge utile de requête VOD classique du chiffreur vers le fournisseur de clés DRM, avec une clé de contenu pour toutes les pistes vidéo et une clé de contenu pour toutes les pistes audio :

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="94ce86fb-07ff-4f43-
adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="94ce86fb-07ff-4f43-
adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
  <!-- Playready -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="9a04f079-9840-4286-
ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02" systemId="9a04f079-9840-4286-
ab92-e65be0885f95">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:AudioFilter />
```

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

Exemple de charge utile de réponse VOD avec des clés

L'exemple suivant affiche une charge utile de réponse classique provenant du fournisseur de clés DRM (les valeurs renvoyées ont été raccourcies par [...] pour plus de précision) :

```
<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 - Cryptage des clés de contenu

Si vous le souhaitez, vous pouvez ajouter le chiffrement de clé de contenu à votre implémentation SPEKE. Le chiffrement de la clé de contenu garantit end-to-end en chiffrant les clés de contenu pour le transit, en plus de chiffrer le contenu lui-même. Si vous n'implémentez pas cette fonctionnalité pour votre fournisseur de clés, vous comptez sur le chiffrement de la couche de transport plus sur une authentification solide pour assurer la sécurité.

Pour utiliser le chiffrement de clé de contenu pour les chiffreurs qui s'exécutent dans le cloud AWS, les clients importent des certificats dans AWS Certificate Manager, puis utilisent les ARN de certificat générés pour leurs activités de chiffrement. Le chiffreur utilise les ARN de certificat et le service ACM pour fournir des clés de contenu chiffrées au fournisseur de clés DRM.

Restrictions

SPEKE prend en charge le chiffrement de clé de contenu, comme indiqué dans la spécification DASH-IF CPIX, avec les restrictions suivantes :

- SPEKE ne prend pas en charge la vérification des signatures numériques (XMLDSIG) pour les charges utiles de demandes ou de réponses.
- SPEKE nécessite 2048 certificats RSA.

Ces restrictions sont également répertoriées dansPersonnalisations et contraintes pour la spécification DASH-IF (p. 24).

Implémentation du chiffrement de clé de contenu

Pour fournir un chiffrement de clé de contenu, incluez les éléments suivants dans vos implémentations de fournisseur de clés DRM :

- Traitez l'élément `<cpix:DeliveryDataList>` dans les charges utiles de demande et de réponse.
- Fournissez des valeurs chiffrées dans l'élément `<cpix:ContentKeyList>` des charges utiles de réponse.

Pour plus d'informations sur ces éléments, consultez leSpécification DASH-IF CPIX 2.3.

Exemple d'élément de chiffrement de clé de contenu `<cpix:DeliveryDataList>` dans la charge utile de requête

```
<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>
```

Exemple d'élément de chiffrement de clé de contenu `<cpix:DeliveryDataList>` dans la charge utile de réponse

```
<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>
```

Exemple d'élément de chiffrement de clé de contenu `<cpix:ContentKeyList>` dans la charge utile de réponse

L'exemple suivant illustre le traitement de la clé de contenu chiffrée dans l'élément `<cpix:ContentKeyList>` de la charge utile de réponse. Elle utilise l'élément `<pskc:EncryptedValue>` :

```
<cpix:ContentKeyList>
     <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
         <cpix:Data>
             <pskc:Secret>
                 <pskc:EncryptedValue>
                     <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
                     <enc:CipherData>
                         <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
                     </enc:CipherData>
                 </pskc:EncryptedValue>
                 <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
             </pskc:Secret>
         </cpix:Data>
     </cpix:ContentKey>
 </cpix:ContentKeyList>
```

En comparaison, l'exemple suivant affiche une charge utile de réponse similaire avec la clé de contenu non chiffrée, comme une clé en clair. Elle utilise l'élément `<pskc:PlainValue>` :

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

API SPEKE v2 - Remplacer l'identificateur de clé

Le chiffreur crée un nouvel identifiant de clé (KID) chaque fois qu'il effectue une rotation des clés. Il transmet le KID au fournisseur de clés DRM dans ses demandes. Le fournisseur de clés répond presque toujours à l'aide du même KID, mais il peut fournir une autre valeur pour le KID dans la réponse.

Voici un exemple de demande avec le KID `11111111-1111-1111-1111-111111111111` :

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" 
 kid="11111111-1111-1111-1111-111111111111" commonEncryptionScheme="cbcs"></
cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- Widevine -->
  <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111" systemId="edef8ba9-79d6-4ace-
a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

La réponse suivante remplace le KID par `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>
```

Licence

Licence publique internationale Creative Commons Attribution - Partager les mêmes formes que 4.0

En exerçant les Droits concédés sous licence (tels que définis ci-dessous), Vous acceptez d'être lié par les conditions générales de la présente Licence publique internationale Creative Commons Attribution - ShareAlike 4.0 (la « Licence publique »). Dans la mesure où cette Licence publique peut être interprétée comme un contrat, Vous bénéficiez des Droits concédés sous licence compte tenu de Votre acceptation des présentes conditions générales et le Concédant Vous accorde ces droits en considération des avantages qu'il a à rendre le Support sous licence disponible dans le cadre des présentes conditions générales.

Article 1 - Définitions.

a. « Support adapté » désigne un support soumis à des Droits d'auteur et autres Droits similaires, dérivé de ou basé sur le Support sous licence et dans lequel le Support sous licence est traduit, altéré, réorganisé, transformé ou autrement modifié d'une manière qui nécessite une autorisation en vertu des Droits d'auteur et Droits similaires détenus par le Concédant. Aux fins de la présente Licence publique, lorsque le Support sous licence est une œuvre musicale, une représentation ou un enregistrement audio, un Support adapté est toujours produit dès lors que le Support sous licence est synchronisé dans une relation temporelle avec une image animée.
b. « Licence d'adaptation » désigne la licence que Vous appliquez à vos Droits d'auteur et Droits similaires dans Vos contributions au Support adapté en accord avec les conditions générales de cette Licence publique.
c. Licence compatible BY-SA désigne une licence répertoriée sur creativecommons.org/compatiblelicenses, approuvée par Creative Commons comme étant essentiellement l'équivalent de cette licence publique.
d. « Droits d'auteur et Droits similaires » désignent des droits d'auteur et/ou des droits similaires étroitement associés à des droits d'auteur, y compris, sans s'y limiter, les droits de représentation, d'émission, d'enregistrement audio et de base de données sui generis, sans égard à l'étiquetage ou à la classification de ces droits. Dans le cadre de la présente Licence publique, les droits spécifiés dans les Alinéas 2 (b) (1) et (2) ne sont pas considérés comme des Droits d'auteur et Droits similaires.
e. « Mesures technologiques effectives » désignent les mesures qui, en l'absence d'autorité compétente, ne peuvent être contournées en vertu de la législation couvrant les obligations de l'Article 11 du traité de l'OMPI sur les droits d'auteur adopté le 20 décembre 1996 et/ou d'accords internationaux similaires.
f. « Exceptions et restrictions » désigne une utilisation équitable, un traitement équitable et/ou toute autre exception ou restriction des Droits d'auteur et Droits similaires qui s'applique à votre Utilisation du Support sous licence.
g. Les éléments de licence désigne les attributs de licence répertoriés dans le nom d'une licence publique Creative Commons. Les éléments de licence de cette licence publique sont Attribution et ShareAlike.
h. « Support sous licence » désigne l'œuvre artistique ou littéraire, la base de données ou tout autre support à laquelle/auquel le Concédant a appliqué cette Licence publique.
i. « Droits concédés sous licence » désigne les droits qui Vous sont octroyés conformément aux conditions de la présente Licence publique, lesquels sont limités à tous les Droits d'auteur et Droits similaires qui s'appliquent à Votre utilisation du Support sous licence et que le Concédant est en droit de concéder sous licence.
j. « Concédant » désigne la ou les personne(s) ou entité(s) qui accordent des droits en vertu de la présente Licence publique.

k. « Partager » signifie fournir un support au public par quelque moyen ou procédé qui requiert une autorisation en vertu des Droits concédés sous licence, tel que la reproduction, l'affichage public, la représentation publique, la distribution, la diffusion, la communication ou l'importation, et rendre le support disponible au public, y compris par des moyens permettant aux membres du public d'accéder au support au lieu et au moment qu'ils auront personnellement choisis.

l. « Droits de base de données sui generis » désigne les droits autres que les droits d'auteur résultant de la Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 sur la protection juridique des bases de données, telle que modifiée et/ou remplacée, ainsi que les autres droits essentiellement équivalents n'importe où dans le monde.

m. « Vous » désigne la personne ou l'entité(s) qui exerce les Droits concédés sous licence en vertu de la présente Licence publique. Votre/Vos a la même signification.

Article 2 - Champ d'application.

a. Octroi de licence.

1. Conformément aux conditions générales de la présente Licence publique, le Concédant Vous accorde une licence mondiale, non exclusive, irrévocable, libre de droits et permettant l'octroi d'une sous-licence pour faire valoir les Droits concédés sous licence sur le Support sous licence dans le but de :

   A. reproduire et Partager le Support sous licence, en tout ou partie ; et

   B. produire, reproduire et Partager le Support adapté.

2. Exceptions et restrictions. Pour éviter toute confusion, lorsque des Exceptions et restrictions s'appliquent à Votre utilisation, la présente Licence publique ne s'applique pas, et Vous n'êtes pas dans l'obligation de vous conformer à ses conditions générales.

3. Durée. La durée de la présente Licence publique est spécifiée dans l'Alinéa 6 (a).

4. Supports et formats ; modifications techniques autorisées. Le Concédant Vous autorise à exercer les Droits concédés sous licence sur tous supports et dans tous formats, actuellement connus ou appelés à être ultérieurement créés, à apporter les modifications techniques nécessaires dans un tel but. Le Concédant renonce et/ou s'engage à ne faire valoir aucun droit ni aucune autorité visant à Vous interdire d'apporter les modifications techniques nécessaires pour l'exercice des Droits concédés sous licence, y compris les modifications techniques nécessaires pour contourner des Mesures technologiques effectives. Dans le cadre de la présente Licence publique, de simples modifications dans les conditions autorisées par le présent Alinéa 2(a)(4) n'ont jamais pour effet de produit un Support adapté.

5. Destinataires en aval.

   A. Offre du Concédant - Support sous licence. Chaque destinataire du Support sous licence reçoit automatiquement une offre du Concédant pour l'exercice des Droits concédés sous licence selon les conditions générales de la présente Licence publique.

   B. Offre supplémentaire du Concédant - Support adapté. Chaque destinataire de Support adapté de votre part reçoit automatiquement une offre du Concédant pour l'exercice des Droits concédés sous licence sur le Support adapté dans les conditions de la Licence de l'adaptateur que Vous appliquez.

   C. Absence de restrictions en aval. Vous n'êtes autorisé ni à proposer ou imposer de conditions supplémentaires ou différentes sur le Support sous licence, ni à appliquer des Mesures technologiques effectives sur ledit Support sous licence, étant entendu que le non-respect de cette clause limite l'exercice des Droits concédés sous licence pour tout destinataire du Support sous licence.

6. Absence d'approbation. Aucune disposition de la présente Licence publique ne saurait constituer ou être interprétée comme une autorisation d'affirmer ou d'insinuer que Vous ou Votre utilisation du Support sous licence bénéficiez d'un quelconque lien, soutien agrément ou statut officiel impliquant une relation avec le Concédant ou d'autres personnes désignées pour recevoir l'attribution prévue à l'Alinéa 3(a)(1)(A)(i).

b. Autres droits.

1. Les droits moraux, tels que le droit à l'intégrité, ne sont pas couverts par la présente Licence publique, de même que les droits de publicité, de confidentialité et/ou autres droits de personnalité similaires ; cependant, dans la mesure du possible, le Concédant renonce et/ou s'engage à ne pas faire valoir de tels droits qui lui seraient concédés dans les limites nécessaires pour Vous permettre d'exercer les Droits concédés sous licence, et dans nulle autre condition.
2. Les droits sur les brevets et les marques commerciales ne sont pas couverts par la présente Licence publique.
3. Dans la mesure du possible, le Concédant renonce à tout droit de percevoir des redevances de Votre part au titre de l'exercice des Droits concédés sous licence, aussi bien par des moyens directs que par le biais d'une société de gestion collective dans le cadre de tout régime de licence réglementaire ou obligatoire, volontaire ou opposable. Dans tous les autres cas, le Concédant se réserve expressément le droit de percevoir de telles redevances.

Article 3 - Conditions de licence.

Votre exercice des Droits concédés sous licence est expressément soumis aux conditions suivantes.

a. Attribution.
   1. Si Vous Partagez le Support sous licence (y compris dans sa forme modifiée), Vous devez :
      A. conserver les éléments suivants s'ils sont fournis par le Concédant avec le Support sous licence :

```
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. indiquer si Vous avez modifié le Support sous licence et conserver une preuve de toute modification antérieure ; et
      C. indiquer que le Support sous licence est soumis à cette Licence publique, et inclure le texte de ladite Licence publique ou incorporer l'URI ou le lien hypertexte renvoyant à cette Licence publique.
   2. Vous pouvez remplir les conditions de l'Alinéa 3(a)(1) par tout moyen raisonnable, selon le support, le moyen et le contexte avec/dans lequel Vous Partagez le Support sous licence. Par exemple, il peut être raisonnable de remplir les conditions en fournissant un URI ou un lien hypertexte renvoyant à une ressource qui inclut les informations requises.
   3. À la demande du Concédant, le cas échéant, Vous devez supprimer toutes les informations requises par l'Alinéa 3(a)(1)(A) dans la mesure du possible.
b. Partagez les mêmes. En plus des conditions de l'Alinéa 3 (a), si Vous Partagez du Support adapté que Vous produisez, les conditions suivantes s'appliquent également.
   1. La licence de l'adaptateur que vous demandez doit être une licence Creative Commons avec les mêmes éléments de licence, cette version ou ultérieure, ou une licence compatible BY-SA.
   2. Vous devez inclure le texte de la Licence de l'adaptateur que vous appliquez ou incorporer l'URI ou le lien hypertexte renvoyant à la Licence de l'adaptateur Vous pouvez remplir cette condition de toute

manière raisonnable, selon le support, le moyen et le contexte dans lequel Vous Partagez du Support adapté.

3. Vous n'êtes autorisé ni à proposer ou imposer de conditions supplémentaires ou différentes sur le Support adapté, ni à appliquer des Mesures technologiques effectives sur ledit Support adapté qui limite l'exercice des Droits accordés en vertu de la Licence de l'adaptateur que Vous appliquez.

Article 4 - Droits de base de données sui generis.

Lorsque les Droits concédés sous licence comprennent des Droits de base de données sui generis qui s'appliquent à Votre utilisation du Support sous licence :

a. Pour éviter toute confusion, l'Alinéa 2 (a) (1) Vous accorde le droit d'extraire, de réutiliser, de reproduire et de Partager l'ensemble ou une grande partie du contenu de la base de données ;
b. si Vous incluez l'ensemble ou une grande partie du contenu de la base de données dans une base de données sur laquelle Vous possédez des Droits de base de données sui generis, la base de données sur laquelle Vous disposez de Droits de base de données sui generis (mais pas son contenu individuel) est considérée comme un Support adapté, notamment aux fins de l'Alinéa 3 (b) ; et
c. Vous êtes tenu de satisfaire aux conditions de l'Alinéa 3(a) si Vous Partagez l'ensemble ou une grande partie du contenu de la base de données. Pour éviter toute confusion, le présent Article 4 complète et ne se substitue pas à Vos obligations qui découlent de la présente Licence publique lorsque les Droits concédés sous licence incluent des Droits d'auteur et droits similaires.

Article 5 - Exclusion de garanties et limitation de responsabilité.

a. Sauf disposition contraire accordée séparément par le Concédant, dans la mesure du possible, le Concédant fournit le Support sous licence en l'état et dans la mesure de ses disponibilités, et ne fait aucune déclaration ou garantie de quelque nature que ce soit concernant le Support sous licence, qu'elle soit explicite, implicite, légale ou autre. Ceci inclut, sans s'y limiter, les garanties de titre, de qualité marchande, d'adéquation à un usage particulier, de non-contrefaçon, d'absence de défauts latents ou autres, d'exactitude ou de présence ou d'absence d'erreurs, qu'elles soient ou non connues ou détectables. Lorsque les exclusions de garanties ne sont pas autorisées en tout ou partie, la présente exclusion de garantie peut ne pas s'appliquer à Votre cas.
b. Dans la mesure du possible, le Concédant décline toute responsabilité envers Vous, quelle que soit la doctrine de droit invoquée (y compris, sans s'y limiter, la négligence) ou en cas de dommages directs, particuliers, indirects, accessoires, consécutifs, punitifs, exemplaires ou autres pertes, coûts, dépenses ou dommages résultant de la présente Licence publique ou de l'utilisation du Support sous licence, même si le Concédant a été informé de la possibilité de telles pertes, coûts, dépenses ou dommages. Lorsqu'une limite de responsabilité n'est pas autorisée en tout ou partie, la présente restriction peut ne pas s'appliquer à Votre cas.
c. L'exclusion de garanties et la limitation de responsabilité mentionnées ci-dessus doivent être interprétées d'une manière qui, dans la mesure du possible, se rapproche le plus d'une exclusion et d'une exonération absolues de toute responsabilité.

Article 6 - Durée et résiliation.

a. La présente Licence publique s'applique pendant la durée des Droits d'auteur et droits similaires concédés aux termes des présentes. Tout manquement de Votre part à vous conformer à la présente Licence publique conduira cependant automatiquement à la résiliation des droits qui Vous sont consentis en vertu des présentes.
b. En cas de résiliation de Votre droit d'utiliser le Support sous licence dans les conditions de l'Alinéa 6(a), ce droit est rétabli :
   1. automatiquement à la date à laquelle la violation est corrigée, sous réserve que cette violation soit corrigée dans les 30 jours suivant la découverte de la violation ; ou
   2. après réintégration expressément faite par le Concédant.

c. Pour éviter toute confusion, le présent Alinéa 6(b) ne remet en cause aucun droit que le Concédant pourrait chercher à faire valoir pour corriger toute violation de la présente Licence publique de Votre part.
d. Pour éviter toute confusion, le Concédant peut également soumettre le Support sous licence à d'autres conditions distinctes ou cesser de distribuer le Support sous licence à tout moment, étant entendu toutefois qu'un tel recours ne saurait nullement mettre fin à la présente Licence publique.
e. Les Articles 1, 5, 6, 7 et 8 demeurent applicables après la fin de la présente Licence publique.

Article 7 - Autres conditions générales.

a. Sauf autorisation contraire, le Concédant ne peut être lié à des conditions supplémentaires ou différentes communiquées par Vos soins.
b. Tout arrangement, accord ou entente eu égard au Support sous licence qui ne serait pas expressément spécifié aux présentes est considéré comme distinct et indépendant des conditions générales de la présente Licence publique.

Article 8 - Interprétation.

a. Pour éviter toute confusion, la présente Licence publique n'entend pas réduire, limiter, restreindre ou imposer de quelconques conditions sur toute utilisation du Support sous licence qui pourrait être faite de manière illicite sans autorisation dans le cadre de cette Licence publique, et ne saurait être interprétée comme telle.
b. Dans la mesure du possible, si une disposition de la présente Licence publique est réputée inapplicable, celle-ci doit être automatiquement réformée dans la stricte mesure où cela est nécessaire pour la rendre applicable. Si ladite disposition ne peut être réformée, elle doit être dissociée de cette Licence publique, sans remettre en cause l'applicabilité des autres conditions générales.
c. Il n'est permis de déroger à aucune condition de la présente Licence publique et aucun manquement à se conformer auxdites conditions ne peut être consenti, sauf accord contraire du Concédant.
d. Aucune condition de la présente Licence publique ne constitue ou ne peut être interprétée comme une restriction ou une renonciation à tout privilège et à toute immunité dont Vous et le Concédant pouvez bénéficier, y compris dans le cadre de procédures judiciaires de toute juridiction ou autorité.

Historique du document

Le tableau suivant décrit les modifications apportées à la documentation SPEKE.

SPEKE v1

Modification	Description	Date
Matrice de support - AWS Elemental Delta	Ajout d'une matrice de support AWS Elemental Delta.	7 février 2019
Mises à jour des fournisseurs de plateforme DRM	Ajout de liens et d'informations relatives aux nouveaux partenaires à la liste des fournisseurs de plateforme DRM.	24 janvier 2019
Chiffreurs tiers inclus	Mise à jour de l'architecture et des descriptions pour prendre en compte les chiffreurs tiers.	20 novembre 2018
Chiffrement de clé de contenu	Ajout de l'option permettant de chiffrer des clés de contenu. Auparavant, Secure Packager et Encoder Key Exchange prenaient uniquement en charge la livraison de clés en clair.	30 octobre 2018
Matrice de support - AWS Elemental Live	Ajout d'une matrice de support AWS Elemental Live.	le 27 septembre 2018
Composants de charge utile standard	Ajout d'une section qui définit les principaux éléments dans la charge utile JSON.	le 27 septembre 2018
Remplacement de l'identifiant de clé (KID)	Ajout d'une section sur le remplacement de l'identifiant de clé (KID) par un fournisseur de clés.	le 27 septembre 2018
Correction des liens vers le site DASH-IF	Correction des liens vers le site DASH IF pour la spécification CPIX et pour la page des ID système.	le 27 septembre 2018
Exemplaire de version pour AWS Elemental Live	Mise à jour de la documentation SPEKE pour inclure les produits AWS Elemental.	20 juillet 2018
CMAF	Mise à jour des tableaux matriciels de support des services pour inclure le format Common Media Application Format (CMAF).	27 juin 2018

Modification	Description	Date
Première version	Première version de Secure Packager and Encoder Key Exchange (SPEKE) version 1, une spécification pour la communication entre un chiffreur de contenu et un fournisseur de clés DRM. Le fournisseur de clés DRM utilise une API Secure Packager et Encoder Key Exchange pour traiter les demandes de clés entrantes.	27 novembre 2017

SPEKE v2

Modification	Description	Date
Mises à jour des fournisseurs de plateforme DRM et section Contrat de chiffrement	Ajout de nouveaux partenaires qualifiés à la colonne SPEKE v2 de la liste des fournisseurs de plateforme DRM. Ajout de deux nouveaux exemples de contrats de chiffrement et de résolution SD max à 1024 x 576 dans tous les exemples concernés.	27 janvier 2022
Première version	Première version de Secure Packager and Encoder Key Exchange (SPEKE) version 2.0, une spécification pour la communication entre un chiffreur de contenu et un fournisseur de clés DRM. Le fournisseur de clés DRM utilise une API Secure Packager et Encoder Key Exchange pour traiter les demandes de clés entrantes.	7 septembre 2021

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le glossaire AWS dans la Référence générale d'AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.