Guide pour les partenaires et les clients

Spécification de l'échange de clés d'encapsulage et d'encodeur sécurisés API

Spécification de l'échange de clés d'encapsulage et d'encodeur sécurisés API: Guide pour les partenaires et les clients

Table of Contents

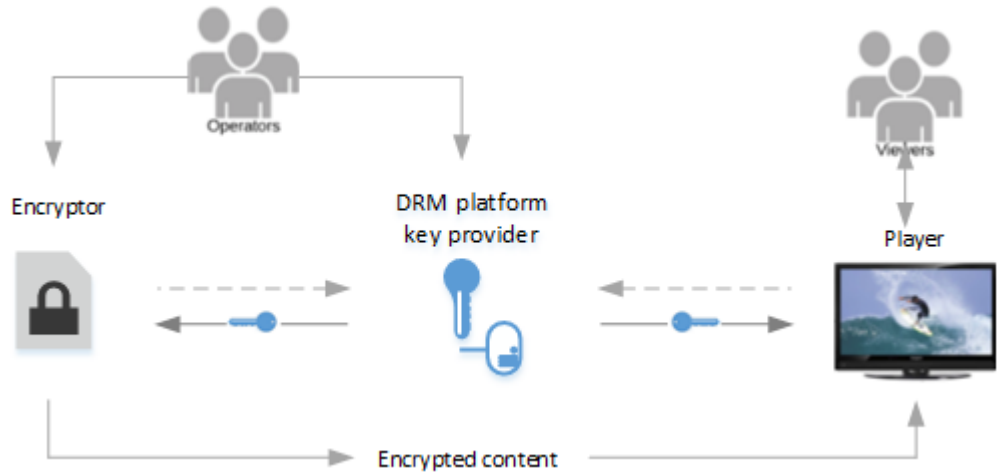
Qu'est-ce que Secure Packager and Encoder Key Exchange ?

Secure Packager and Encoder Key Exchange (SPEKE) définit la norme de communication entre les crypteurs et les packagers de contenu multimédia et les fournisseurs de clés de gestion des droits numériques ()DRM. La spécification s'adapte aux crypteurs exécutés sur site et dans le AWS cloud.

Rubriques

Architecture générale

L'illustration suivante présente une vue d'ensemble de l'architecture de chiffrement de SPEKE contenu pour les produits sur site.



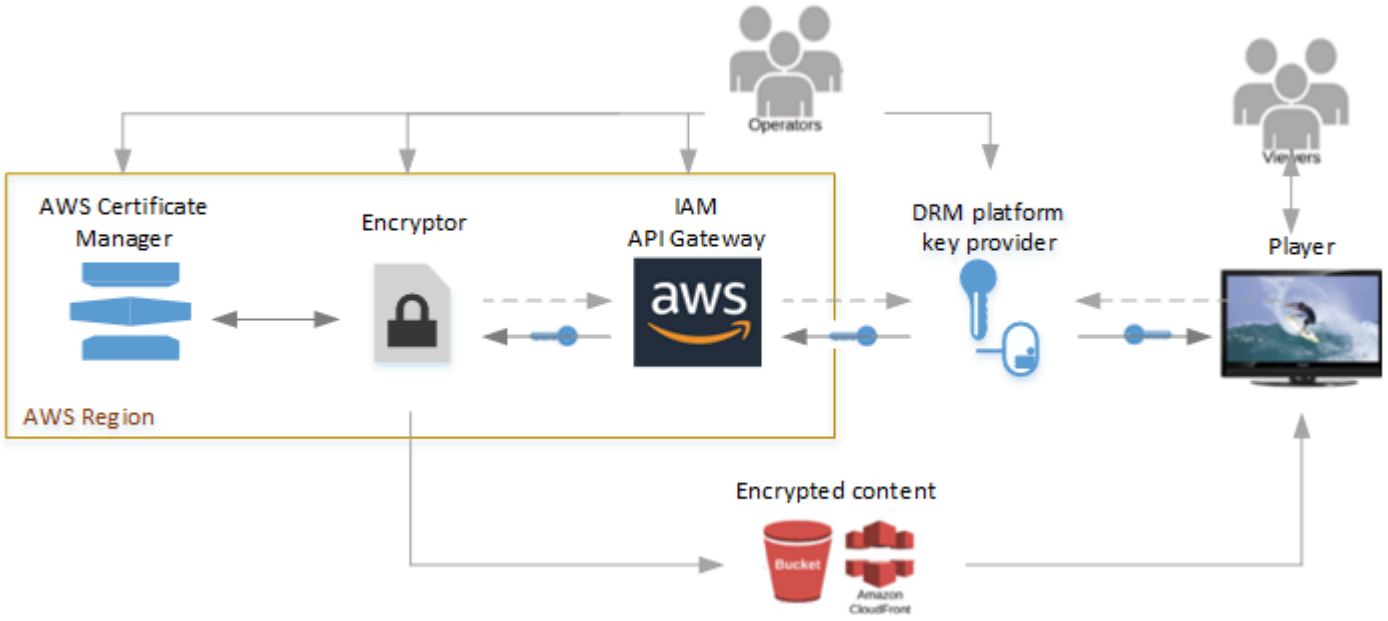
Voici les principaux composants de l'architecture précédente :

- Encrypteur — Fournit la technologie de cryptage. Reçoit les demandes de chiffrement de son opérateur et récupère les clés requises auprès du fournisseur de DRM clés pour sécuriser le contenu crypté.

- DRMfournisseur de clés de plate-forme — Fournit des clés de chiffrement au crypteur via un système SPEKE compatibleAPI. Le fournisseur fournit également des licences aux lecteurs multimédias pour le déchiffrement.
- Joueur : demande des clés au même fournisseur de clés de DRM plateforme, que le joueur utilise pour déverrouiller le contenu et le diffuser à ses spectateurs.

AWSarchitecture basée sur le cloud

L'illustration suivante montre l'architecture de haut niveau lorsqu'elle SPEKE est utilisée avec des services et des fonctionnalités exécutés dans le AWS cloud.



Voici les principaux services et composants :

- Encrypteur — Fournit la technologie de cryptage dans le AWS cloud. Le crypteur reçoit les demandes de son opérateur et récupère les clés de chiffrement requises auprès du fournisseur de DRM clés, via Amazon API Gateway, pour sécuriser le contenu crypté. Il fournit le contenu chiffré à un compartiment Amazon S3 ou via une CloudFront distribution Amazon.
- AWSIAMet Amazon API Gateway : gère les rôles fiables des clients et les communications par proxy entre le crypteur et le fournisseur de clés. APIGateway fournit des fonctionnalités de journalisation et permet aux clients de contrôler leurs relations avec le crypteur et avec la DRM plateforme. Les clients autorisent l'accès aux principaux fournisseurs via la configuration des IAM rôles. APILa passerelle doit résider dans la même AWS région que le crypteur.

- AWSCertificate Manager — (facultatif) Assure 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 résider dans la même AWS région que le crypteur.
- DRMfournisseur de clés de plate-forme — Fournit des clés de chiffrement au crypteur via un système SPEKE compatibleAPI. Le fournisseur fournit également des licences aux lecteurs multimédias pour le déchiffrement.
- Joueur : demande des clés au même fournisseur de clés de DRM plateforme, que le joueur utilise pour déverrouiller le contenu et le diffuser à ses spectateurs.

Comment démarrer

Pour des informations d'introduction supplémentaires sur SPEKE le sujet, voir Êtes-vous nouveau dans le domaine SPEKE ? .

Êtes-vous un client ?

Associez-vous à un fournisseur de DRM plateforme AWS Elemental pour configurer l'utilisation du chiffrement. Pour plus de détails, consultez la section Intégration des clients.

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

Exposez un REST API pour votre principal fournisseur conformément aux SPEKE spécifications. Pour plus de détails, voir les SPEKEAPIspécifications.

Vous débutez avec SPEKE ?

Cette section fournit des informations d'introduction aux lecteurs qui découvrent Secure Packager et Encoder Key Exchange ()SPEKE.

Pour une présentationSPEKE, regardez la webémission suivante :

Informations et spécifications de service associées

- APIautorisations de passerelle — Comment contrôler l'accès à une autorisation API avec AWS Identity and Access Management (AWSIAM).
- AWS AssumeRole— Comment utiliser le AWS Security Token Service (AWSSTS) pour assumer la fonctionnalité des rôles.
- AWSSigv4 — Comment signer une HTTP demande à l'aide de Signature Version 4.
- DASHCPIX-Spécification IF v2.0 — La version de spécification DASH -IF Content Protection Information Exchange Format (CPIX), sur laquelle cette spécification SPEKE v1.0 est basée.
- DASHCPIX-Spécification IF v2.3 — La version de spécification DASH -IF Content Protection Information Exchange Format (CPIX), sur laquelle cette spécification SPEKE v2.0 est basée.
- DASH-Système IF IDs — Liste des identifiants enregistrés pour DRM les systèmes.
- https://github.com/awslabs/speke-reference-server— Exemple de fournisseur de clés de référence à utiliser avec votre AWS compte, pour vous aider à démarrer une SPEKE implémentation dansAWS.

Terminologie

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

- ARN— Nom de la ressource Amazon. Identifie une AWS ressource de manière unique.
- Clé de contenu : clé cryptographique utilisée pour chiffrer une partie du contenu.
- Fournisseur de contenu : éditeur qui fournit les droits et les règles nécessaires à la diffusion de contenus multimédias protégés. Le fournisseur de contenu peut également fournir un support source (format mezzanine, pour le transcodage), des identifiants de ressources, des identificateurs

clés (KIDs), des valeurs clés, des instructions de codage et des métadonnées de description du contenu.

- DRM— Gestion des droits numériques. Utilisé pour protéger le contenu numérique protégé par des droits d'auteur contre un accès non autorisé.
- DRMplate-forme : système qui fournit des DRM fonctionnalités et une assistance aux crypteurs et aux visionneurs de contenu, notamment en fournissant des DRM clés et des licences pour le chiffrement et le déchiffrement du contenu.
- DRMfournisseur — Voir DRM plateforme.
- DRMsystème — Norme pour les DRM mises en œuvre. Les DRM systèmes courants incluent Apple FairPlay, Google Widevine et Microsoft. PlayReady DRMles fournisseurs de contenu utilisent des systèmes pour sécuriser le contenu numérique destiné à être diffusé aux spectateurs et à permettre aux spectateurs d'y accéder. Pour obtenir la liste des DRM systèmes enregistrés avec DASH -IF, voir DASH-IF system. IDs La CPIXspécification DASH -IF utilise le terme « DRM système » tel que défini ici et, à certains endroits, elle utilise le terme « DRM système » pour désigner ce que cette spécification appelle une DRM plate-forme.
- DRMsolution — Voir DRM plateforme.
- DRMtechnologie — Voir DRM système.
- Crypteur : composant de traitement multimédia qui chiffre le contenu multimédia à l'aide de clés obtenues auprès du fournisseur de clés. Les crypteurs ajoutent généralement également des signaux de DRM chiffrement et des métadonnées au support. Les chiffreurs sont généralement des encodeurs, des empaqueteurs et des transcodeurs.
- Fournisseur de clés : composant d'une DRM plate-forme qui expose un SPEKE REST API pour traiter les demandes 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 DRM plate-forme qui gère les clés pour le chiffrement et le déchiffrement du contenu.
- Opérateur : personne chargée de faire fonctionner l'ensemble du système, y compris le crypteur et le fournisseur de clés.
- Lecteur : lecteur multimédia fonctionnant pour le compte d'un téléspectateur. Obtient ses informations à partir de différentes sources, notamment les fichiers manifestes multimédia, les fichiers multimédias et les DRM licences. Demande des licences à la DRM plateforme au nom des spectateurs.

Accueil des clients pour SPEKE

Protégez votre contenu contre toute utilisation non autorisée en associant un fournisseur de clés de gestion des droits numériques (SPEKE) Secure Packager and Encoder Key Exchange (DRM) à votre crypteur et à vos lecteurs multimédias. SPEKEdéfinit la norme de communication entre les crypteurs et les conditionneurs de contenu multimédia et les fournisseurs de clés de gestion des droits numériques (DRM). Pour participer, vous choisissez un fournisseur de clés de DRM plateforme et configurez la communication entre le fournisseur de clés et vos crypteurs et lecteurs.

Rubriques

Commencez avec un fournisseur DRM de plateforme

Les partenaires Amazon suivants fournissent des implémentations de DRM plateformes tierces pourSPEKE. 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 n'ont actuellement pas de page Amazon Partner Network, mais vous pouvez les contacter directement. Les partenaires peuvent vous aider à vous préparer à utiliser leurs plateformes.

DRMfournisseur de plateforme	SPEKEsupport v1	SPEKEsupport v2
Axinom	√	√
Acheter DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKAréseaux	√	√
Cloud Insys DRM	√	√

DRMfournisseur de plateforme	SPEKEsupport v1	SPEKEsupport v2
Intertrust Technologies	√	√
Irdeto	√	√
Joueur JW	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKEsupport en matière de AWS services et de produits

Cette section répertorie le SPEKE support fourni par AWS les services multimédias exécutés dans le AWS cloud et par les produits multimédias AWS sur site. Ces services et produits sont les crypteurs de l'architecture de chiffrement du SPEKE contenu. Vérifiez que votre protocole de diffusion et le DRM système que vous souhaitez sont disponibles pour votre service ou produit.

AWSservice ou produit	SPEKEsupport v1	SPEKEsupport v2	DRMTechnologies prises en charge
AWSElemental MediaConvert - Service qui s'exécute dans le cloud AWS	√	√	Documentation
AWSElemental MediaPackage -	√	√	Documentation

AWSservice ou produit	SPEKEsupport v1	SPEKEsupport v2	DRMTechnologies prises en charge
Service qui s'exécute dans le cloud AWS			
AWSElemental Live - Produit sur site	√		Documentations : MPEG- DASH/HLS
AWSElemental Server - Produit sur site	√		Documentation

SPEKEassistance en matière de services et de produits destinés aux AWS partenaires

Cette section répertorie le SPEKE support fourni par les services et produits AWS partenaires qui s'exécutent dans le AWS cloud. Ces services et produits sont les crypteurs de l'architecture de chiffrement du SPEKE contenu. Vérifiez que votre protocole de diffusion et le DRM système que vous souhaitez sont disponibles pour votre service ou produit.

AWSservice ou produit	SPEKEsupport v1	SPEKEsupport v2	DRMTechnologies prises en charge
Encodage vidéo Bitmovin Live	√		Documentation
Codage vidéo à la demande Bitmovin () VOD	√		Documentation

SPEKEAPIspécification

Il s'agit de la REST API spécification pour Secure Packager et Encoder Key Exchange ()SPEKE. Utilisez cette spécification pour protéger les DRM droits d'auteur des clients qui utilisent le chiffrement.

Dans un flux de travail de streaming vidéo, le moteur de chiffrement communique avec le fournisseur de clés de DRM plate-forme 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 du document pour un end-to-end chiffrement plus sécurisé.

Cette spécification répond aux objectifs suivants :

- Définissez une interface simple, fiable et hautement sécurisée que DRM les fournisseurs et les clients peuvent utiliser pour intégrer les chiffreurs lorsque le chiffrement du contenu est requis.
- Couvrez VOD les flux de travail en direct, et incluez les conditions d'erreur et les mécanismes d'authentification nécessaires à une communication robuste et hautement sécurisée entre les crypteurs et les points de terminaison des DRM principaux fournisseurs.
- Incluez le support pourHLS,MSS, et le DASH packaging et leurs DRM systèmes communs : FairPlay, PlayReady, et Widevine/CENC.
- Veillez à ce que les spécifications soient simples et extensibles, afin de prendre en charge DRM les futurs systèmes.
- Utilisez un simple RESTAPI.

> **Note**
>
>

OU ARISINGFROM, OUT OF CONNECTION WITH THIS MATERIAL OU IN THE USE OR OTHER DEALINGS OF THISMATERIAL.

Rubriques

Authentification requise pour SPEKE

SPEKEnécessite une authentification pour les produits sur site et pour les services et fonctionnalités exécutés dans le AWS cloud.

Rubriques

Authentification pour les implémentations AWS dans le cloud

SPEKEnécessite une AWS authentification par le biais de IAM rôles à utiliser avec un crypteur. IAMles rôles sont créés par le DRM fournisseur ou par l'opérateur propriétaire du DRM point de terminaison dans un AWS compte. Chaque rôle se voit attribuer un Amazon Resource Name (ARN), que l'opérateur du service AWS Elemental fournit sur la console de service lorsqu'il demande le chiffrement. Les autorisations de politique du rôle doivent être configurées pour autoriser l'accès au fournisseur de clés API et aucun autre accès aux AWS ressources. Lorsque le crypteur contacte le fournisseur de DRM clés, il utilise ce rôle ARN pour assumer le rôle de titulaire du compte du fournisseur de clés, qui renvoie des informations d'identification temporaires que le crypteur peut utiliser pour accéder au fournisseur de clés.

Une implémentation courante consiste pour l'opérateur ou le fournisseur de DRM plate-forme à utiliser Amazon API Gateway devant le fournisseur clé, puis à activer AWS l'autorisation Identity and Access Management (AWSIAM) 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 de la API passerelle :

```
{
    "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 montre un rôle ARN créé pour accéder au fournisseur de DRM clés :

```
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 AWSSigv4.

Authentification pour les produits sur site

Pour les produits sur site, nous vous recommandons d'utiliser l'authentificationSSL/TLSet digest pour une sécurité optimale, mais vous devez au minimum utiliser l'authentification de base. HTTPS

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

- Authentification Digest — L'en-tête d'autorisation se compose de l'identifiant `Digest` suivi d'une série de valeurs qui authentifient la demande. Plus précisément, une valeur de réponse est générée par le biais d'une série de fonctions de MD5 hachage qui incluent un one-time-use nonce unique provenant du serveur qui est utilisé pour garantir que le mot de passe circule en toute sécurité.

- Authentification de base — L'en-tête d'autorisation se compose de l'identifiant `Basic` suivi d'une chaîne codée en base 64 qui représente le nom d'utilisateur et le mot de passe, séparés par deux points.

Pour plus d'informations sur l'authentification de base et l'authentification par condensé, y compris des informations détaillées sur l'en-tête, consultez la spécification RFC2617 de l'Internet Engineering Task Force (IETF) intitulée HTTP Authentication : authentification d'accès de base et condensé.

SPEKEAPIv1

Il s'agit de REST API la version v1 de Secure Packager and Encoder Key Exchange (SPEKE). Utilisez cette spécification pour protéger les DRM droits d'auteur des clients qui utilisent le chiffrement. Pour être SPEKE conforme, votre fournisseur de DRM clés doit exposer les informations REST API décrites dans cette spécification. Le crypteur passe des API appels à 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 SPEKE implémentation complète.

SPEKEutilise la définition de structure de données du 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 pour fournir un DRM échange multiple extensible entre la DRM plate-forme et le crypteur. 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 à débit adaptatif incluent HLSDASH, etMSS.

Pour des informations détaillées sur le format d'échange, consultez les CPIX spécifications du DASH Industry Forum à l'adresse https://dashif.org/docs/ DASH -IF- CPIX -v2-0.pdf.

Rubriques

- SPEKEAPIv1 - Personnalisations et contraintes de la spécification DASH -IF
- SPEKEAPIv1 - Composants de charge utile standard
- SPEKEAPIv1 - Exemples d'appels de méthodes de flux de travail en direct

- SPEKEAPIv1 - exemples d'appels VOD de méthodes de flux de travail
- SPEKEAPIv1 - Chiffrement des clés de contenu
- SPEKEAPIv1 - Rythme cardiaque
- SPEKEAPIv1 - Remplacer l'identifiant de clé

SPEKEAPIv1 - Personnalisations et contraintes de la spécification DASH -IF

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

- SPEKE suit le flux de travail Encryptor Consumer.
- Pour les clés de contenu chiffrées, les restrictions suivantes SPEKE s'appliquent :
  - SPEKEne prend pas en charge la vérification de signature numérique (XMLDSIG) pour les charges utiles de demande ou de réponse.
  - SPEKEnécessite des certificats RSA basés sur 2048.
- Pour la rotation des flux de travail clés, SPEKE nécessite le `ContentKeyUsageRule` filtre,`KeyPeriodFilter`. SPEKEignore tous les autres `ContentKeyUsageRule` paramètres.
- SPEKE omet la fonctionnalité `UpdateHistoryItemList`. Si la liste est présente dans la réponse, l'SPEKEignore.
- SPEKEprend en charge la rotation des touches. SPEKEutilise uniquement le `ContentKeyPeriod@index pour suivre la période clé.
- Pour prendre en charge MSS PlayReady, SPEKE utilise un paramètre personnalisé sous la `DRMSystem` balise,`SPEKE:ProtectionHeader`.
- Pour le HLS packaging, si le `URIExtXKey` est présent dans la réponse, celle-ci doit contenir les données complètes à ajouter dans le URI paramètre du `EXT-X-KEY` tag d'une HLS playlist, sans autre exigence de signalisation.
- Pour la HLS playlist, sous la `DRMSystem` balise, SPEKE fournit les paramètres personnalisés facultatifs `speke:KeyFormat` et`speke:KeyFormatVersions`, pour les valeurs de la `EXT-X-KEY` balise, les `KEYFORMATVERSIONS` paramètres `KEYFORMAT` et.

  Le vecteur HLS d'initialisation (IV) suit toujours le numéro de segment, sauf indication explicite de 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.
- SPEKEne prend actuellement pas en charge plusieurs pistes ou clés par contenu.

  Le SPEKE crypteur compatible agit en tant que client et envoie les `POST` opérations au 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.

SPEKEAPIv1 - Composants de charge utile standard

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

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

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

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

Identifiant	Description
`systemId` ou `schemeId`	Identifiant unique pour le type de DRM système, tel qu'il est enregistré auprès de

Identifiant	Description
	l'organisation DASH IF. Pour une liste, voir DASH-IF System. IDs
`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 (PSSH). Ce type d'en-tête contient une référence aux `kid` données personnal isées du DRM fournisseur`systemID`, dans le cadre de 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 suivant montre une partie d'une demande d'exemple envoyée par le crypteur au fournisseur de DRM clés, dont les principaux composants sont mis en évidence. La première demande concerne une clé standard, tandis que la seconde demande concerne une PSSH réponse :

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

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

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

_Exemples de réponses pour la clé standard et pour PSSH _

L'exemple suivant montre la réponse correspondante du fournisseur de DRM clés au crypteur :

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

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

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

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

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

SPEKEAPIv1 - Exemples d'appels de méthodes de flux de travail en direct

Exemple de syntaxe de la requête

Ce qui suit URL est un exemple qui n'indique pas un format fixe :

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

Corps de la demande

Un CPIX élément.

En-têtes de requête

Nom	Type	Se produit	Description
`AWS Authorization`	Chaîne	1..1	Voir AWSSigv4

Nom	Type	Se produit	Description
`X-Amz-Security-Token`	Chaîne	1..1	Voir AWSSigv4
`X-Amz-Date`	Chaîne	1..1	Voir AWSSigv4
`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

HTTP CODE	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	DASH- réponse à la CPIX charge utile
`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 plus d'informations sur la façon d'ajouter le chiffrement par clé de contenu, consultez la section Chiffrement par clé de contenu.

Exemple de charge utile de requête en direct avec des clés

L'exemple suivant montre une charge utile typique d'une demande en direct envoyée par le crypteur au fournisseur de DRM clés :

```
<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 montre une charge utile de réponse typique du fournisseur de DRM clés :

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

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

```
  </cpix:DRMSystem>

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

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

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

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

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

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

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

SPEKEAPIv1 - exemples d'appels VOD de méthodes de flux de travail

Exemple de syntaxe de la requête

Ce qui suit URL est un exemple et n'indique pas un format fixe.

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

Corps de la demande

Un CPIX élément.

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

HTTP CODE	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	DASH- réponse à la CPIX charge utile
`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 plus d'informations sur la façon d'ajouter le chiffrement par clé de contenu, voir Chiffrement par clé de contenu.

VODExemple de charge utile de demande avec des clés en clair

L'exemple suivant montre une charge utile de VOD requête de base envoyée par le crypteur au fournisseur de DRM clés :

```
<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>
```

VODExemple de charge utile de réponse avec des clés en clair

L'exemple suivant montre une charge utile de VOD réponse de base provenant du fournisseur de DRM clés :

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

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

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

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

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

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

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

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

SPEKEAPIv1 - Chiffrement des clés de contenu

Vous pouvez éventuellement ajouter le chiffrement par clé de contenu à votre SPEKE implémentation. Le chiffrement des clés de contenu garantit end-to-end une protection complète en chiffrant les clés de contenu pour le transit, en plus du chiffrement du contenu lui-même. Si vous ne l'implémentez pas pour votre fournisseur de clés, vous comptez sur le chiffrement de la couche de transport associé à une authentification forte pour des raisons de sécurité.

Pour utiliser le chiffrement par clé de contenu pour les chiffreurs exécutés dans AWS le Cloud, les clients importent des certificats dans le AWS Certificate Manager, puis utilisent le certificat obtenu ARNs pour leurs activités de chiffrement. Le crypteur utilise le certificat ARNs et le ACM service pour fournir des clés de contenu chiffrées au fournisseur de DRM clés.

Restrictions

SPEKEprend en charge le chiffrement des clés de contenu tel que spécifié dans la CPIX spécification DASH -IF avec les restrictions suivantes :

- SPEKEne prend pas en charge la vérification de signature numérique (XMLDSIG) pour les charges utiles de demande ou de réponse.
- SPEKEnécessite des certificats RSA basés sur 2048.

Ces restrictions sont également répertoriées dans Personnalisations et contraintes de la spécification DASH -IF.

Implémentation du chiffrement de clé de contenu

Pour assurer le chiffrement des clés de contenu, incluez les éléments suivants dans les implémentations de votre fournisseur de DRM clés :

- 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 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>
```

SPEKEAPIv1 - Rythme cardiaque

Exemple de syntaxe de la requête

Ce qui suit URL est un exemple qui n'indique pas un format fixe :

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

Réponse à la requête

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

SPEKEAPIv1 - Remplacer l'identifiant de clé

Le crypteur crée un nouvel identifiant de clé (KID) chaque fois qu'il fait pivoter les clés. Il le transmet KID au fournisseur DRM clé dans ses demandes. Presque toujours, le fournisseur de clés répond de la même manièreKID, mais il peut fournir une valeur différente pour le KID dans la réponse.

Voici un exemple de demande contenant 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 la réponse KID à `22222222-2222-2222-2222-222222222222` :

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

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

SPEKEAPIv2

Il s'agit de REST API la version v2 de Secure Packager and Encoder Key Exchange (SPEKE). Utilisez cette spécification pour protéger les DRM droits d'auteur des clients qui utilisent le chiffrement. Pour être SPEKE conforme, votre fournisseur de DRM clés doit exposer les informations REST API décrites dans cette spécification. Le crypteur passe des API appels à 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 SPEKE implémentation complète.

SPEKEutilise la définition de structure de données du 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 pour fournir un DRM échange multiple extensible entre la DRM plate-forme et le crypteur. 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 à débit adaptatif incluent HLSDASH, etMSS.

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

D'un SPEKE côté, cela est appliqué par l'utilisation de l'`X-Speke-Version`HTTPen-tête, et sur le CPIX côté par l'utilisation de l'`CPIX@version`attribut. L'absence de ces éléments dans les demandes est typique des anciens flux de travail de la version SPEKE 1. Dans les flux de travail SPEKE v2, le fournisseur de clés est censé traiter CPIX les documents uniquement s'il prend en charge les deux paramètres de version.

Pour des informations détaillées sur le format d'échange, consultez la spécification DASH Industry Forum CPIX 2.3.

Globalement, la SPEKE v2.0 apporte les évolutions suivantes par rapport à SPEKE la v1.0 :

- Toutes les balises de l'espace de SPEKE XML noms sont déconseillées au profit de balises équivalentes dans l'espace de noms CPIX XML
- `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 CPIX attributs obligatoires :`CPIX@version`, `ContentKey@commonEncryptionScheme`
- Nouvel CPIX élément optionnel : `DRMSystem.ContentProtectionData`
- Support pour plusieurs clés de contenu
- Mécanisme de versionnement croisé entre et SPEKE CPIX
- HTTPévolution des en-têtes : nouvel `X-Speke-Version` en-tête, `Speke-User-Agent` en-tête renommé en `X-Speke-User-Agent`
- Dépréciation du rythme cardiaque API

Comme la spécification de la SPEKE version 1.0 reste inchangée, les implémentations existantes n'ont pas besoin de changer pour continuer à prendre en charge les flux de travail de la version SPEKE 1.0.

Rubriques

SPEKEAPIv2 - Personnalisations et contraintes de la spécification DASH -IF

La spécification DASH Industry Forum CPIX 2.3 prend en charge un certain nombre de cas d'utilisation et de topologies. La spécification SPEKE API v2.0 définit à la fois un CPIX profil et un API pourCPIX. Afin d'atteindre ces deux objectifs, il respecte le CPIX cahier des charges avec les personnalisations et contraintes suivantes :

CPIXProfil

- SPEKE suit le flux de travail Encryptor Consumer.
- Pour les clés de contenu chiffrées, les restrictions suivantes SPEKE s'appliquent :
  - SPEKEne prend pas en charge la vérification de signature numérique (XMLDSIG) pour les charges utiles de demande ou de réponse.
  - SPEKEnécessite des certificats RSA basés sur 2048.
- SPEKEne tire parti que d'un sous-ensemble de CPIX fonctionnalités :
  - SPEKE omet la fonctionnalité `UpdateHistoryItemList`. Si la liste est présente dans la réponse, l'SPEKEignore.
  - SPEKEomet la fonctionnalité de touche root/feuille. Si l'`ContentKey@dependsOnKey`attribut est présent dans la réponse, il l'SPEKEignore.

  - SPEKEomet l'`BitrateFilter`élément et l'`VideoFilter@wcg`attribut. Si ces éléments ou attributs sont présents dans la CPIX charge utile, l'SPEKEignore.
- Seuls les éléments ou attributs référencés comme « pris en charge » sur la page des composants de charge utile standard ou sur la page du contrat de chiffrement peuvent être utilisés dans les CPIX documents échangés avec la SPEKE version 2.
- Lorsqu'ils sont inclus dans une CPIX demande par le crypteur, tous les éléments et attributs doivent porter une valeur valide dans la CPIX réponse du fournisseur de clés. Dans le cas contraire, le crypteur doit s'arrêter et générer une erreur.
- SPEKEprend en charge la rotation des touches avec `KeyPeriodFilter` des éléments. SPEKEutilise uniquement le `ContentKeyPeriod@index` pour suivre la période clé.
- Pour HLS la signalisation, plusieurs `DRMSystem.HLSSignalingData` éléments doivent être utilisés : un avec une valeur d'`DRMSystem.HLSSignalingData@playlist`attribut « media » et un autre avec une valeur d'`DRMSystem.HLSSignalingData@playlist`attribut « master ».
- 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 crypteur doit inclure une valeur pour l'`CPIX@contentId`attribut. Lorsqu'il reçoit une valeur vide pour cet attribut, le fournisseur de clés renvoie une erreur avec la description « Missing CPIX @ contentId ». `CPIX@contentId`la valeur ne peut pas être remplacée par le fournisseur de clés.

  `CPIX@id`la valeur, si elle n'est pas nulle, doit être ignorée par le fournisseur de clés.
- Le crypteur doit inclure une valeur pour l'`CPIX@version`attribut. Lorsqu'il reçoit une valeur vide pour cet attribut, le fournisseur de clés renvoie une erreur avec la description « Missing CPIX @version ». Lors de la réception d'une demande avec une version non prise en charge, la description de l'erreur renvoyée par le fournisseur de clés doit être « Unsupported @version »CPIX.

  `CPIX@version`la valeur ne peut pas être remplacée par le fournisseur de clés.
- Le crypteur doit inclure une valeur pour l'`ContentKey@commonEncryptionScheme`attribut pour chaque clé demandée. Lorsqu'il reçoit une valeur vide pour cet attribut, le fournisseur de clés renvoie une erreur avec la description « Missing ContentKey @ commonEncryptionScheme for KID `id` ».

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

Les `ContentKey@commonEncryptionScheme` valeurs ne sont pas toutes compatibles avec toutes les DRM technologies. À 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.

- Lors de la réception de valeurs différentes pour `DRMSystem@PSSH` XML `<pssh>` un élément `DRMSystem.ContentProtectionData` interne dans le corps de la CPIX réponse, le crypteur doit s'arrêter et générer une erreur.

API pour CPIX

- Le fournisseur de clés doit inclure une valeur pour l'en-tête de `X-Speke-User-Agent` HTTP réponse.
- Un SPEKE crypteur conforme agit en tant que client et envoie les POST opérations au point de terminaison du fournisseur de clés.
- Le crypteur doit inclure une valeur pour l'en-tête de la `X-Speke-Version` HTTP demande, avec la SPEKE version utilisée avec la demande, formulée sous MajorVersion la forme. MinorVersion, comme « 2.0 » pour la SPEKE version 2.0. Si le fournisseur de clés ne prend pas en charge la SPEKE version utilisée par le crypteur pour la demande en cours, il doit renvoyer une erreur avec la description « SPEKE Version non prise en charge » et ne pas essayer de traiter le CPIX document de son mieux.

  La valeur `X-Speke-Version` d'en-tête définie par le crypteur ne peut pas être modifiée par le fournisseur de clés en réponse à la demande.
- Lorsqu'il reçoit des erreurs dans le corps de la réponse, le crypteur doit générer une erreur et ne pas réessayer la demande avec un versionnage SPEKE v1.0.

  Si le fournisseur de clés ne renvoie pas d'erreur mais ne renvoie pas un CPIX document contenant les informations obligatoires, le crypteur doit s'arrêter et générer une erreur.

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

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

SPEKEAPIv2 - Composants de charge utile standard

Par le biais d'une seule SPEKE demande, le crypteur 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 CPIX document standard est composé de trois sections de liste obligatoires, plus une section de liste facultative pour la rotation des clés de contenu en direct.

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

Il s'agit d'une section obligatoire, pertinente à la fois pour le live et le VOD streaming, qui définit les différentes clés de contenu qui doivent être utilisées par le crypteur. L'`<cpix:ContentKeyList>`élément peut contenir un ou plusieurs éléments `<cpix:ContentKey>` enfants, chacun d'eux décrivant une clé de contenu distincte.

Conformément à la CPIX spécification, les valeurs possibles de l'`ContentKey@commonEncryptionScheme`attribut sont définies dans la spécification du chiffrement commun dans les fichiers au format de fichier multimédia de ISO base (ISO/IEC23001-7:2016) :

- 'cenc' : AES - CTR mode cryptage complet de l'échantillon et du sous-échantillon vidéo NAL
- 'cbc1' : AES - CBC mode cryptage de l'échantillon complet et du sous-échantillon vidéo NAL
- 'cens' : AES - CTR mode cryptage partiel des modèles vidéo NAL
- 'cbcs' : AES - CBC mode cryptage partiel du modèle vidéo NAL

L'exemple suivant montre un CPIX document 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 crypteur en incluant l'élément<cpix : >. DeliveryDataList Reportez-vous à la section Chiffrement de la clé de contenu pour plus de détails.

Élément soutenu par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments obligatoires pour les enfants	Éléments enfants facultatifs
<pixels : >CPIX	contentId, version, xmlns : cpix, xmlns : pskc	nom, xmlns:enc	un <cpix : ContentKeyList >, un<cpix : >, un <cpix : DRMSystem List > ContentKeyUsageRuleList	un <cpix : DeliveryDataList >, un <cpix : >ContentKeyPeriodList
<pixels : >ContentKeyList	-	id	au moins un <cpix : >ContentKey	-
<pixels : >ContentKey	enfant commonEncryptionScheme, Données	id, Algorithme, ExplicItiv	un <pskc:Secret>	-
<pskc:Secret>	PlainValue ou EncryptedValue	Valeur MAC	-	<enc : EncryptionMethod >, <enc : >CipherData

<cpix : >section DRMSystemList

Il s'agit d'une section obligatoire, pertinente à la fois pour le live et le VOD streaming, qui définit les différents DRM systèmes à exploiter ainsi que les clés de contenu.

L'exemple suivant montre une liste de DRM systèmes avec une seule spécification PlayReady DRM système :

```
<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 une liste complète DRMsystemIDs, reportez-vous à la section Protection du contenu du référentiel DASH -IF Identifiers.

Élément soutenu par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments obligatoires pour les enfants	Éléments enfants facultatifs
<pixels : >DRMSystemList	-	id	au moins un <cpix : >DRMSystem	-
<pixels : >DRMSystem	enfant, systemId	identifiant, nom, PSSH	-	ContentProtectionData SmoothStreamingProtectionHeaderData, deux éléments <cpix : HLSSignalingData > avec une valeur d'attribut de playlist différente

DRMSystem@PSSHest obligatoire si ISO l'BMFFencapsulation est appliquée aux segments multimédia. DRMSystem.ContentProtectionDataXML<pssh>l'élément interne est utilisé par le crypteur uniquement à des fins de signalisation manifeste.

S'il DRMSystem@PSSH est présent et DRMSystem.ContentProtectionData contient un XML <pssh> élément interne, les deux valeurs doivent être identiques.

Si DRMSystem la signalisation doit être transportée dans des HLS manifestes, les <cpix:HLSSignalingData playlist="master"> éléments a <cpix:HLSSignalingData playlist="media"> et a doivent être inclus dans la CPIX demande et la réponse.

<cpix : >section ContentKeyPeriodList

Il s'agit d'une section facultative, pertinente uniquement pour la diffusion en direct, qui définit les périodes cryptographiques appliquées au contenu.

L'<cpix:ContentKeyPeriodList>élément peut contenir un ou plusieurs éléments <cpix:ContentKeyPeriod> enfants, chacun d'eux décrivant une période cryptographique distincte dans la chronologie en temps réel. L'utilisation dans le UUIDs cadre 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 soutenu par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments obligatoires pour les enfants	Éléments enfants facultatifs
<pixels : >ContentKeyPeriodList	-	id	au moins un <cpix : >ContentKeyPeriod	-
<pixels : >ContentKeyPeriod	identifiant, index	-	-	-

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

<cpix : >section ContentKeyUsageRuleList

Il s'agit d'une section obligatoire, pertinente à la fois pour le live et pour le VOD streaming, qui définit comment les différentes clés de contenu protégeront les pistes au sein du streamset et pendant les périodes de chiffrement.

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

L'exemple suivant montre une liste simple avec une seule règle appliquant 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 soutenu par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments obligatoires pour les enfants	Éléments enfants facultatifs
<pixels : >ContentKeyUsageRuleList	-	id	au moins un <cpix : >ContentKeyUsageRule	-
<pixels : >ContentKeyUsageRule	enfant, intendedTrackType	-	au moins un <cpix : AudioFilter > ou un	<pixels : >KeyPeriodFilter

Élément soutenu par SPEKE	Attributs obligatoires	Attributs facultatifs	Éléments obligatoires pour les enfants	Éléments enfants facultatifs
			<cpix : >(*) VideoFilter	
<pixels : >KeyPeriodFilter	periodId	-	-	-
<pixels : >AudioFilter	-	minChannels, maxChannels	-	-
<pixels : >VideoFilter	-	minPixels ,maxPixels, elleminFps, maxFps	-	-

(*) Pour une explication détaillée de l'utilisation d'une ou de plusieurs clés de contenu pour protéger une ou plusieurs pistes d'un streamset, reportez-vous à la section de documentation du contrat de chiffrement. _

SPEKEAPIv2 - Contrat de chiffrement

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

Bien qu'il s'agisse d'une bonne pratique recommandée par le secteur, l'utilisation de plusieurs clés de contenu pour les différentes pistes d'un stream n'est pas obligatoire, mais recommandée : au moins deux clés de contenu différentes, une pour les pistes audio et l'autre pour les pistes vidéo. Il est possible d'utiliser une seule clé de contenu pour chiffrer plusieurs pistes, mais cela doit être explicitement indiqué dans le CPIX document envoyé par le crypteur au fournisseur de clés. D'une manière générale, le crypteur décrit toujours précisément le nombre de clés de contenu requises et la manière dont elles sont utilisées pour chiffrer les différentes pistes multimédias.

Principes

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

- un `ContentKeyUsageRule@intendedTrackType` attribut qui peut référencer un ou plusieurs sous-composants, séparés par le signe « + » si plusieurs sous-composants sont utilisés. La valeur de `ContentKeyUsageRule@intendedTrackType` doit être unique dans un contrat de chiffrement et ne peut pas être utilisée dans plusieurs `ContentKeyUsageRule` éléments.
- un ou plusieurs éléments `<cpix:AudioFilter>` ou éléments `<cpix:VideoFilter>` enfants, selon la valeur de `ContentKeyUsageRule@intendedTrackType` l'attribut.

Les règles régissant cette relation sont les suivantes :

- Lorsque toutes les pistes audio et vidéo du streamset doivent être protégées par une clé de contenu unique, la chaîne `'ALL'` doit être utilisée comme valeur d'`ContentKeyUsageRule@intendedTrackType`attribut. L'exemple 1 illustre un tel cas d'utilisation. Dans ce cas, les éléments a `<cpix:AudioFilter />` `<cpix:VideoFilter />` et a sans attribut doivent être inclus. Toute autre combinaison `<cpix:AudioFilter>` et/ou `<cpix:VideoFilter>` élément n'est pas valide dans ce contexte particulier.
- Pour tous les autres cas d'utilisation, la valeur de l'`ContentKeyUsageRule@intendedTrackType`attribut peut être définie librement, et le nombre d'éléments `<cpix:AudioFilter />` et un élément `<cpix:VideoFilter />` enfant 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 la valeur de l'attribut. `ContentKeyUsageRule@intendedTrackType` L'exemple 8 l'illustre lorsque plusieurs sous-composants sont utilisés : il `ContentKeyUsageRule@intendedTrackType="SD+HD"` est décrit par deux éléments `<cpix:VideoFilter>` enfants distincts avec des valeurs d'attributs différentes, et `ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"` est décrit par trois éléments `<cpix:VideoFilter>` enfants distincts avec des valeurs d'attributs différentes.

Filtres

CPIXdéfinit plusieurs éléments et attributs de filtrage, mais n'SPEKEen prend en charge qu'un sous-ensemble. Le tableau suivant résume ces différences :

CPIXtype de filtre	SPEKESupport global	Attributs de filtre pris en charge par SPEKE	Attributs de filtre non pris en charge par SPEKE
<pixels : >VideoFilter	Oui	minPixels,maxPixels, hdr,minFps, maxFps (attributs facultatifs)	wcg
<pixels : >AudioFilter	Oui	minChannels, maxChannels (attributs facultatifs)	
<pixels : >KeyPeriodFilter	Oui	periodId (attribut obligatoire)	
<pixels : >BitrateFilter	Non	N/A	N/A
<pixels : >LabelFilter	Non	N/A	N/A

Conformément à la CPIX spécification de VideoFilter, [minPixels,maxPixels] est une plage complète dans les deux dimensions, tandis que (minFps,maxFps] n'inclut que la maxFps dimension. Car 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 crypteur et le fournisseur de clés se comportent de manière appropriée et garantissent une protection adéquate du contenu. Le tableau suivant présente le comportement recommandé dans ces situations :

Dans cette situation	Le crypteur devrait/doit...	Le principal fournisseur devrait/doit...
Aucune règle ne s'applique à une ou plusieurs pistes du streamset (voir exemple 3 ci-dessous)	Le crypteur doit examiner sa configuration (externe à la CPIX charge utile) et vérifier que les pistes concernées ne nécessitent pas de cryptage.	Non pertinent : le fournisseur principal ne connaît pas la structure du stream set.

Dans cette situation	Le crypteur devrait/doit...	Le principal fournisseur devrait/doit...
	Si ce n'est pas le cas, le crypteur devrait générer une erreur et arrêter le traitement.	
Plusieurs règles se chevauchent et suggèrent plusieurs clés de contenu pour chiffrer une piste spécifique	Le crypteur doit appliquer la dernière valeur évaluée ContentKeyUsageRule avec succès dans l'ordre du document.	Non pertinent : le fournisseur principal ne connaît pas la structure du stream set.
Le contrat de chiffrement change en un seul cycle de SPEKE demande/réponse	Le crypteur 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 reproduise en premier lieu, le fournisseur de clés ne doit pas modifier un contrat de chiffrement reçu dans la CPIX charge utile de la SPEKE demande.
Contrat de chiffrement mal formé : exception à la contrainte de cardinalité intendedTrackType /Filters, filtres ou attributs non pris en charge	Le crypteur doit déclencher une exception, arrêter le traitement et ne pas envoyer la SPEKE demande au fournisseur de clés, car cela entraînerait très probablement une protection du contenu erronée ou laisserait certaines traces non protégées.	Le fournisseur de clés doit déclencher une exception et renvoyer une erreur « Contrat de chiffrement mal formé ».

Dans cette situation	Le crypteur devrait/doit...	Le principal fournisseur devrait/doit...
Contrat de chiffrement bien conçu, mais en violation des contraintes liées aux niveaux de DRM sécurité : par exemple, une clé de contenu unique est demandée pour protéger à la fois les pistes audio et les pistes UHD vidéo	Si le crypteur a connaissance des contraintes liées aux niveaux de DRM sécurité, il doit déclencher une exception, arrêter le traitement et ne pas envoyer la SPEKE demande au fournisseur de clés, car cela entraînerait très probablement une protection du contenu erronée.	Le fournisseur de clés doit déclencher une exception et renvoyer le message d'erreur « Contrat de CPIX chiffrement demandé non pris en charge ».
Contrat de chiffrement manquant	Le crypteur ne doit pas envoyer de CPIX documents qui ne contiennent aucun AudioFilter élément VideoFilter ou élément.	Le fournisseur de clés doit déclencher une exception et renvoyer une erreur « Contrat de CPIX chiffrement manquant ».

Exemples de contrats de chiffrement

Exemple 1 : une clé 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 clé 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 cryptées

```
<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 clés de contenu pour différentes pistes vidéo (SD/HD), une clé 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 clés de contenu pour différentes pistes vidéo (SD/HD/UHD), une clé 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 clés de contenu pour différentes pistes vidéo (SD/HD/UHD1/UHD2), une clé 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 clés de contenu pour différentes pistes vidéo (SD///HD1/HD2UHD1/UHD2), une clé 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 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-->
 <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 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>
```

SPEKEAPIv2 - Exemples d'appels de méthodes de flux de travail en direct

Exemple de syntaxe de la requête

Ce qui suit URL est un exemple qui n'indique pas un format fixe :

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

Corps de la demande

Un CPIX document.

En-têtes de requête

Nom	Type	Se produit	Description
`AWS Authorization`	Chaîne	1..1	Voir AWSSigv4

Nom	Type	Se produit	Description
`X-Amz-Security-Token`	Chaîne	1..1	Voir AWSSigv4
`X-Amz-Date`	Chaîne	1..1	Voir AWSSigv4
`Content-Type`	Chaîne	1..1	application/xml
`X-Speke-Version`	Chaîne	1..1	SPEKEAPIversion utilisée avec la demande, formulée sous la forme MajorVersion. MinorVersion, comme « 2.0 » pour la SPEKE version 2.0

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
`X-Speke-Version`	Chaîne	1..1	SPEKEAPIversion utilisée avec la demande, formulée sous la forme MajorVersion. MinorVersion, comme « 2.0 » pour la SPEKE version 2.0

Réponse à la requête

HTTP CODE	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	DASH- réponse à la CPIX charge utile
`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 plus d'informations sur la façon d'ajouter le chiffrement par clé de contenu, voir Chiffrement par clé de contenu.

Exemple de charge utile de requête en direct avec des clés

L'exemple suivant montre une charge utile typique d'une demande en direct envoyée par le crypteur au fournisseur de DRM clés, 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 montre une charge utile de réponse typique du fournisseur de DRM clés (les valeurs renvoyées ont été raccourcies avec [...] pour des raisons de lisibilité) :

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

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

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

SPEKEAPIv2 - exemples d'appels VOD de méthodes de flux de travail

Exemple de syntaxe de la requête

Ce qui suit URL est un exemple et n'indique pas un format fixe.

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

Corps de la demande

Un CPIX document.

En-têtes de requête

Nom	Type	Se produit	Description
`AWS Authorization`	Chaîne	1..1	Voir AWSSigv4
`X-Amz-Security-Token`	Chaîne	1..1	Voir AWSSigv4

Nom	Type	Se produit	Description
`X-Amz-Date`	Chaîne	1..1	Voir AWSSigv4
`Content-Type`	Chaîne	1..1	application/xml
`X-Speke-Version`	Chaîne	1..1	SPEKEAPIversion utilisée avec la demande, formulée sous la forme MajorVersion. MinorVersion, comme « 2.0 » pour la SPEKE version 2.0

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
`X-Speke-Version`	Chaîne	1..1	SPEKEAPIversion utilisée avec la demande, formulée sous la forme MajorVersion. MinorVersion, comme « 2.0 » pour la SPEKE version 2.0

Réponse à la requête

HTTP CODE	Nom de la charge utile	Se produit	Description
`200 (Success)`	CPIX	1..1	DASH- réponse à la CPIX charge utile
`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 plus d'informations sur la façon d'ajouter le chiffrement par clé de contenu, voir Chiffrement par clé de contenu.

VODExemple de charge utile de demande avec des clés en clair

L'exemple suivant montre une charge utile typique d'une VOD demande envoyée par le crypteur au fournisseur de DRM clés, 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>
```

VODExemple de charge utile de réponse avec des clés en clair

L'exemple suivant montre une charge utile de réponse typique du fournisseur de DRM clés (les valeurs renvoyées ont été raccourcies avec [...] pour des raisons de lisibilité) :

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

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

```
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKEAPIv2 - Chiffrement des clés de contenu

Vous pouvez éventuellement ajouter le chiffrement par clé de contenu à votre SPEKE implémentation. Le chiffrement des clés de contenu garantit end-to-end une protection complète en chiffrant les clés de contenu pour le transit, en plus du chiffrement du contenu lui-même. Si vous ne l'implémentez pas pour votre fournisseur de clés, vous comptez sur le chiffrement de la couche de transport associé à une authentification forte pour des raisons de sécurité.

Pour utiliser le chiffrement par clé de contenu pour les chiffreurs exécutés dans AWS le Cloud, les clients importent des certificats dans le AWS Certificate Manager, puis utilisent le certificat obtenu ARNs pour leurs activités de chiffrement. Le crypteur utilise le certificat ARNs et le ACM service pour fournir des clés de contenu chiffrées au fournisseur de DRM clés.

Restrictions

SPEKEprend en charge le chiffrement des clés de contenu tel que spécifié dans la CPIX spécification DASH -IF avec les restrictions suivantes :

- SPEKEne prend pas en charge la vérification de signature numérique (XMLDSIG) pour les charges utiles de demande ou de réponse.
- SPEKEnécessite des certificats RSA basés sur 2048.

Ces restrictions sont également répertoriées dans Personnalisations et contraintes de la spécification DASH -IF.

Implémentation du chiffrement de clé de contenu

Pour assurer le chiffrement des clés de contenu, incluez les éléments suivants dans les implémentations de votre fournisseur de DRM clés :

- 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 la spécification 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>
```

SPEKEAPIv2 - Remplacer l'identifiant de clé

Le crypteur crée un nouvel identifiant de clé (KID) chaque fois qu'il fait pivoter les clés. Il le transmet KID au fournisseur DRM clé dans ses demandes. Presque toujours, le fournisseur de clés répond de la même manièreKID, mais il peut fournir une valeur différente pour le KID dans la réponse.

Voici un exemple de demande contenant 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 la réponse KID à 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 pour la SPEKE API spécification

Creative Commons Attribution- ShareAlike 4.0 Licence publique internationale

En exerçant les droits sous licence (définis ci-dessous), vous acceptez et acceptez d'être lié par les termes et conditions de cette licence publique internationale Creative Commons Attribution-ShareAlike 4.0 (« 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. La licence de l'adaptateur désigne la licence que vous appliquez à vos droits d'auteur et droits similaires dans le cadre de vos contributions au matériel adapté conformément aux termes et conditions de cette licence publique.

c. Une 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. Par mesures technologiques efficaces, on entend les mesures qui, en l'absence d'une autorité appropriée, ne peuvent être contournées en vertu des lois remplissant les obligations découlant de l'article 11 du Traité sur le WIPO droit 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 désignent les attributs de licence répertoriés dans le nom d'une licence publique Creative Commons. Les éléments de licence de cette licence publique sont l'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 matériel sous licence, en tout ou en partie ; et

   B. produire, reproduire et partager du matériel 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 — Matériel adapté. Chaque destinataire du matériel adapté de votre part reçoit automatiquement une offre du concédant pour exercer les droits sous licence sur le matériel adapté conformément aux conditions de la licence de l'adaptateur que vous demandez.

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 matériel 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. indiquez si vous avez modifié le matériel sous licence et conservez une indication des modifications précédentes ; et

   C. indiquez que le matériel sous licence est sous licence publique et incluez le texte de cette licence publique URI ou un hyperlien vers celle-ci.

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 satisfaire aux conditions en fournissant un lien URI ou un hyperlien vers une ressource contenant 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. ShareAlike. Outre les conditions de la section 3 (a), si vous partagez du matériel 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 une version ultérieure, ou une licence compatible BY-SA.

2. Vous devez inclure le texte URI ou le lien hypertexte de la licence de l'adaptateur que vous demandez. Vous pouvez satisfaire à cette condition de toute manière raisonnable en fonction du support, des moyens et du contexte dans lesquels vous partagez du matériel adapté.
3. Vous ne pouvez pas proposer ou imposer de conditions supplémentaires ou différentes ou appliquer des mesures technologiques efficaces au matériel adapté qui restreignent l'exercice des droits accordés en vertu de la licence d'adaptateur que vous demandez.

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 ambiguïté, la section 2 (a) (1) vous accorde le droit d'extraire, de réutiliser, de reproduire et de partager la totalité ou une partie substantielle du contenu de la base de données ;
b. si vous incluez la totalité ou une partie substantielle du contenu de la base de données dans une base de données dans laquelle vous détenez des droits de base de données sui generis, alors la base de données dans laquelle vous détenez des droits de base de données sui generis (mais pas son contenu individuel) est du matériel adapté, notamment aux fins de la section 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 compter de la date à laquelle la violation est corrigée, à condition qu'elle soit corrigée dans les 30 jours suivant la découverte de la violation ; ou
   2. lors de la réintégration expresse 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 des documents pour le guide SPEKE destiné aux partenaires et aux clients

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

SPEKE v1

Modification	Description	Date
Matrice de support : services et produits des AWS partenair es	Ajout d'une nouvelle section dédiée au SPEKE Support pour les services et produits destinés aux AWS partenair es, répertoriant les services Bitmovin.	13 janvier 2023
Mises à jour destinées aux fournisseurs de DRM plateformes	Des liens et de nouvelles informations sur les partenair es ont été ajoutés à la liste des fournisseurs de la DRM plateforme.	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 ne prenaient en charge que la livraison de clés claires.	30 octobre 2018
Matrice de support - AWS Elemental Live	Ajout d'une matrice de support AWS Elemental Live.	le 27 septembre 2018

Modification	Description	Date
Composants de charge utile standard	Ajout d'une section qui définit les principaux éléments de la JSON charge utile.	le 27 septembre 2018
KIDpasser outre	Ajout d'une section sur KID les dérogations par un fournisseur clé.	le 27 septembre 2018
Liens corrigés vers le site DASH -IF	Corriger les liens vers le site DASH IF pour la CPIX spécification et pour la IDs page système.	le 27 septembre 2018
Copie de publication pour AWS Elemental Live	Mise à jour de la SPEKE documentation pour inclure les produits AWS Elemental.	20 juillet 2018
CMAF	Mise à jour des tableaux de matrice de support pour les services afin d'inclure le format d'application multimédi a commun (CMAF).	27 juin 2018
Première version	Publication initiale de Secure Packager and Encoder Key Exchange (SPEKE) version 1, une spécification pour la communication entre un crypteur de contenu et un DRM fournisseur de clés. Le fournisseur de DRM clés met à disposition un module d'emballage sécurisé et un échange de clés d'encodage API pour traiter les demandes de clés entrantes.	27 novembre 2017

SPEKE v2

Modification	Description	Date
Mises à jour de DRM la section des fournisseurs de plateformes et de la SPEKE section de support des AWS services et produits	Webstream a été ajouté à la colonne SPEKE v2 de la liste des fournisseurs de DRM plateformes, ajouté MediaConvert à la colonne SPEKE v2 du tableau du SPEKE support en matière de AWS services et de produits.	10 octobre 2024
Mises à jour de DRM la section des fournisseurs de plateformes	De nouveaux partenaires qualifiés ont été ajoutés à la colonne SPEKE v2 de la liste des fournisseurs de DRM plateformes.	9 août 2023
Mises à jour des sections d'exemples d'appels VOD de méthodes Live et de flux de travail	Ajout d'un en-tête de X-Speke-Version réponse manquant dans les sections SPEKE v2 Live et d'exemples d'appels de méthodes de VOD flux de travail.	13 janvier 2023
Mises à jour de DRM la section relative aux fournisseurs de plateformes et aux contrats de chiffrement	De nouveaux partenaires qualifiés ont été ajoutés à la colonne SPEKE v2 de la liste des fournisseurs de DRM plateformes. Ajout de deux nouveaux exemples de contrats de chiffrement et modification de la résolution SD max à 1024 x 576 dans tous les exemples concernés.	27 janvier 2022

Modification	Description	Date
Première version	Publication initiale de Secure Packager and Encoder Key Exchange (SPEKE) version 2.0, une spécification pour la communication entre un crypteur de contenu et un DRM fournisseur de clés. Le fournisseur de DRM clés met à disposition un module d'emballage sécurisé et un échange de clés d'encodage API pour traiter les demandes de clés entrantes.	7 septembre 2021

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.