合作夥伴和客戶指南

安全封裝器和編碼器金鑰交換API規格

安全封裝器和編碼器金鑰交換API規格: 合作夥伴和客戶指南

Table of Contents

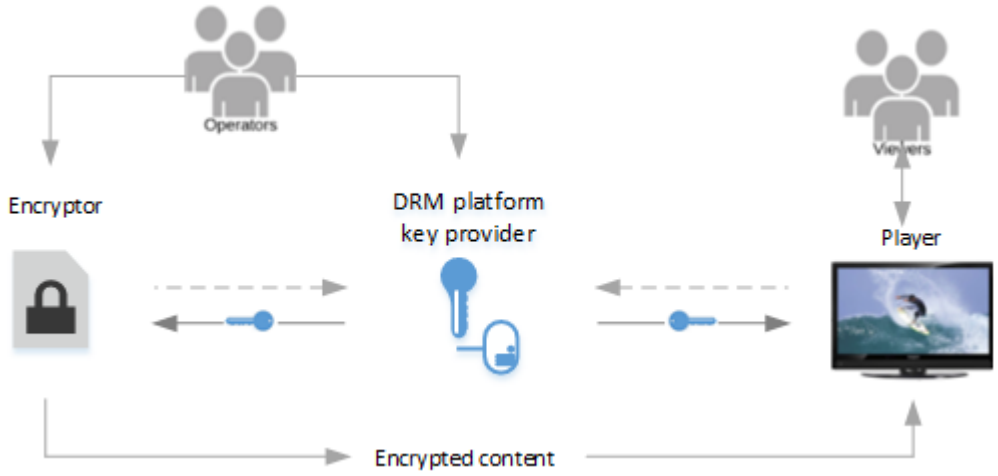
什麼是安全打包器和編碼器密鑰交換？

安全封裝程式和編碼器金鑰交換 (SPEKE) 定義了媒體內容的加密程式與封裝程式與數位版權管理 (DRM) 金鑰提供者之間的通訊標準。該規範可容納在內部部署和雲端中執行的AWS加密器。

主題

一般建築

下圖顯示內部部署產品之內SPEKE容加密架構的高階檢視。

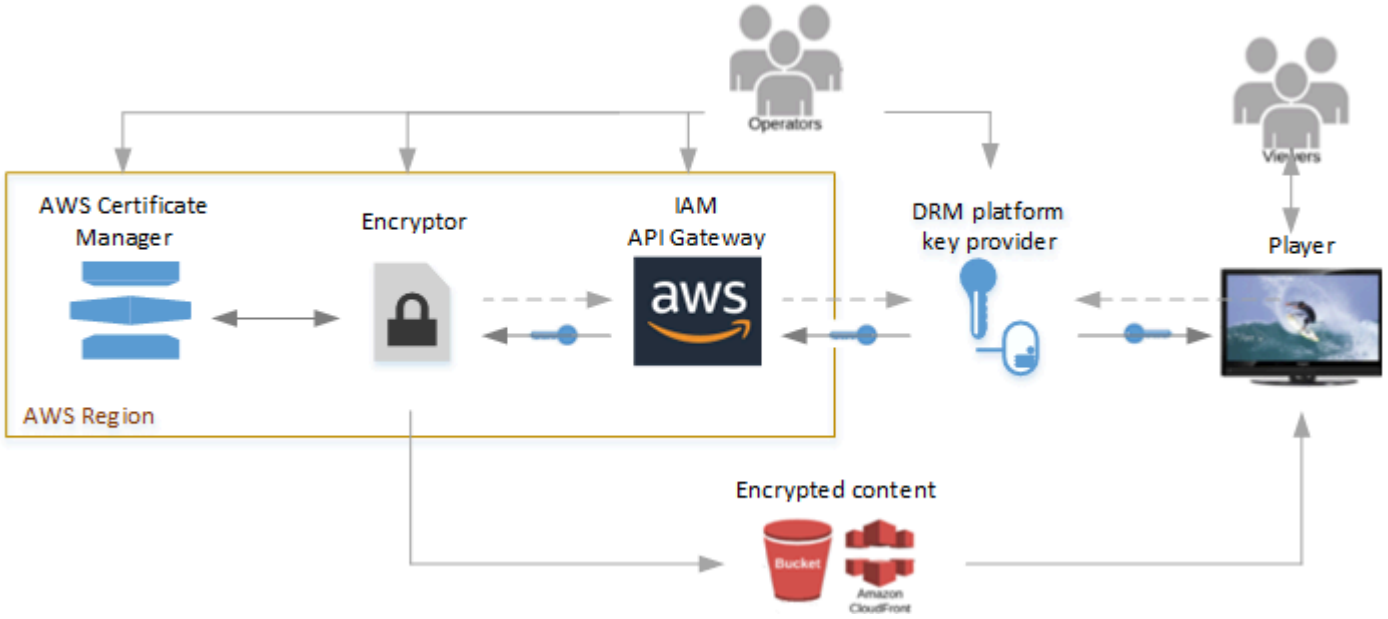


這些是上述架構的主要元素：

- 加密器 — 提供加密技術。接收來自其操作員的加密要求，並從金鑰提供者擷取所需的金DRM鑰，以保護加密內容的安全。
- DRM平台金鑰提供者 — 透過符合 SPEKE-API 規範的加密程式提供加密金鑰。提供者也為媒體播放器提供解密授權。
- 播放程式 — 請求來自同一DRM平台金鑰提供者的金鑰提供者，玩家使用這些金鑰來解除鎖定內容並將其提供給觀眾。

AWS雲端架構

下圖顯示與AWS雲端中執行的服務和功能搭配使用時SPEKE的高階架構。



這些是主要服務和元件：

- 加密器 — 在AWS雲中提供加密技術。加密器會透過 Amazon API Gateway 接收操作員的要求，並從金DRM鑰提供者擷取所需的加密金鑰，以保護加密內容的安全。它將加密的內容交付到 Amazon S3 儲存貯體或透過 Amazon CloudFront 分發。
- AWSIAM和 Amazon API Gateway — 管理加密器和金鑰提供者之間客戶信任的角色和代理通訊。APIGateway 提供記錄功能，並可讓客戶控制與加密程式和DRM平台之間的關係。客戶透過IAM角色設定啟用金鑰提供者存取權。API閘道必須與加密程式位於相同的AWS區域中。
- AWSCer@@ tificate Manager — (選擇性) 提供內容金鑰加密的憑證管理。建議使用加密內容金鑰以保護通訊安全。憑證管理員必須與加密程式位於相同的AWS區域。
- DRM平台金鑰提供者 — 透過符合 SPEKE-API 規範的加密程式提供加密金鑰。提供者也為媒體播放器提供解密授權。
- 播放程式 — 請求來自同一DRM平台金鑰提供者的金鑰提供者，玩家使用這些金鑰來解除鎖定內容並將其提供給觀眾。

如何開始

有關的其他介紹性材料SPEKE，請參閱您是新來SPEKE的嗎？ 。

您是客戶嗎？

與 AWS Elemental 平DRM台供應商合作，設定使用加密功能。如需詳細資訊，請參閱客戶入職。

您是DRM平台供應商還是擁有自己金鑰提供者的客戶？

公開符RESTAPI合SPEKE規範的金鑰提供者。如需詳細資訊，請參閱SPEKEAPI規格。

剛接觸 SPEKE 嗎？

本節為剛接觸安全封裝程式和編碼器金鑰交換 () SPEKE 的讀者提供介紹性資訊。

如需簡介SPEKE，請觀看下列網路廣播：

相關服務資訊及規格

- API閘道權限 — 如何控制對API具有 I AWS dentity and Access Management (AWSIAM) 權限的存取。
- AWS AssumeRole— 如何使用AWS安全性權杖服務 (AWSSTS) 假設角色功能。
- AWSSigv4 — 如何使用簽名版本 4 簽署HTTP請求。
- DASH-IF CPIX 規格 v2.0 — 此 SPEKE 1.0 規範所依據的 DASH-IF 內容保護資訊交換格式 (CPIX) 規格版本。
- DASH-IF CPIX 規格 v2.3 — 此 v SPEKE 2.0 規範所依據的 DASH-IF 內容保護資訊交換格式 (CPIX) 規格版本。
- DASH-IF 系統 IDs — 系統的註冊識別碼清單。DRM
- https://github.com/awslabs/speke-reference-server— 與您的AWS帳戶搭配使用的參考金鑰提供者範例，以協助您開始使用中的SPEKE實作AWS。

術語

下列清單定義此規定中使用的術語。在可能的情況下，此規範遵循 DASH-IF CPIX 規範中使用的術語。

- ARN— Amazon 資源名稱. 唯一識別AWS資源。
- 內容金鑰 — 用於加密部分內容的加密金鑰。
- 內容提供者 — 提供傳遞受保護媒體之權利和規則的發行者。內容供應商也可能提供來源媒體 (Mezzanine 格式，用於轉碼)、資產識別碼、金鑰識別碼 (KIDs)、金鑰值、編碼指示和內容描述中繼資料。
- DRM— 數位版權管理。用於防止版權數位內容未經授權的存取。
- DRM平台 — 一種為內容加密器和觀眾提供DRM功能和支持的系統，包括為內容加密和解密提供密DRM鑰和許可。

- DRM供應商 — 請參閱DRM平台。
- DRM系統-DRM 實施的標準。常見的DRM系統包括蘋果 FairPlay, 谷歌維德文, 和 Microsoft. PlayReady DRM內容供應商會使用系統來保護數位內容的安全，以便傳送給觀眾以及供觀眾存取。如需使用-IF 註冊的DRM系統清單，請參閱 DASH DASH-IF 系統。IDsDASH-IF CPIX 規格使用此處定義的術語「DRMsystem」，在某些地方，它使用「DRM系統」來表示此規範所指的DRM平台。
- DRM解決方案 — 請參閱DRM平台。
- DRM技術 — 見DRM系統.
- 加密器 — 一種媒體處理元件，可使用金鑰提供者取得的金鑰來加密媒體內容。加密器通常還將加DRM密信號和元數據添加到媒體中。加密程式通常是編碼器、封裝器和轉碼器。
- 金鑰提供者 — DRM 平台的元件，可公開處理金鑰要求。SPEKE REST API金鑰提供者可能是金鑰伺服器本身，或可能是平台的另一個元件。
- 金鑰伺服器 — 維護金鑰以進行內容加密和解密的DRM平台元件。
- 操作員 — 負責操作整個系統的人員，包括加密器和金鑰提供者。
- 播放器 — 代表觀眾操作的媒體播放器。從不同來源獲取其信息，包括媒體清單文件，媒體文件和DRM許可證。代表觀眾向DRM平台請求許可證。

的客戶加入 SPEKE

將 Secure Packager 和 Encoder Key Exchange （SPEKE） 數位權利管理 （DRM） 金鑰提供者與您的加密器和媒體播放器結合，保護您的內容不受未經授權的使用。SPEKE 定義媒體內容和數位權利管理 （DRM） 金鑰提供者的加密器和封裝器之間的通訊標準。若要加入，您可以選擇DRM平台金鑰提供者，並設定金鑰提供者與加密者和播放器之間的通訊。

主題

DRM 平台供應商入門

下列 Amazon 合作夥伴為 提供第三方DRM平台實作SPEKE。如需其產品和聯絡方式的詳細資訊，請點選該供應商的 Amazon 合作夥伴網路頁面連結。沒有連結的合作夥伴目前沒有 Amazon Partner Network 頁面，但您可以直接聯絡他們。合作夥伴可以協助您完成設定，以使用其平台。

DRM 平台供應商	SPEKE v1 支援	SPEKE v2 支援
Axinom	√	√
購買DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKA 插圖	√	√
Insys Cloud DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√

DRM 平台供應商	SPEKE v1 支援	SPEKE v2 支援
JW 播放器	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE， Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKE AWS服務與產品的支援

本節列出由在AWS雲端中執行的 AWS Media Services 和AWS內部部署媒體產品提供的SPEKE支援。這些服務和產品是SPEKE內容加密架構中的加密器。確認您的串流通訊協定和您想要DRM的系統可供您的服務或產品使用。

AWS 服務或產品	SPEKE v1 支援	SPEKE v2 支援	支援DRM的技術
AWS Elemental MediaConvert - 在 AWS Cloud 中執行的服務	√	√	文件
AWS Elemental MediaPackage - 在 AWS Cloud 中執行的服務	√	√	文件
AWS Elemental Live - 內部部署產品	√		文件： MPEG-DASH / HLS

AWS 服務或產品	SPEKE v1 支援	SPEKE v2 支援	支援DRM的技術
AWS Elemental Server - 內部部署產品	√		文件

SPEKE AWS合作夥伴服務和產品的支援

本節列出在 AWS Cloud 中執行的AWS合作夥伴服務和產品所提供的SPEKE支援。這些服務和產品是SPEKE內容加密架構中的加密器。確認您的串流通訊協定和您想要DRM的系統可供您的服務或產品使用。

AWS 服務或產品	SPEKE v1 支援	SPEKE v2 支援	支援DRM的技術
Bitmovin Live Video 編碼	√		文件
Bitmovin Video on demand （ VOD ） 編碼	√		文件

SPEKEAPI規格

這是「安全封裝程式」與「編碼器金鑰交換」(SPEKE) 的RESTAPI規格。使用此規格為使用加密的客戶提供DRM版權保護。

在視訊串流工作流程中，加密引擎會與DRM平台金鑰提供者通訊，以要求內容金鑰。這些金鑰具有高度機密，因此金鑰提供者和加密引擎建立高度安全、可信任的通訊通道至關重要。您也可以加密文件中的內容金鑰，以獲得更安全、 end-to-end 加密的功能。

此規定旨在達成下列目標：

- 定義一個簡單、受信任且高度安全的介面，DRM供應商和客戶可以在需要內容加密時與加密器整合。
- 涵蓋VOD和即時工作流程，並包含錯誤狀況和驗證機制，以便在加密程式和DRM金鑰提供者端點之間進行穩健、高度安全的通訊所需。
- 包括對HLSMSS、和DASH封裝及其通用DRM系統的支援： FairPlay PlayReady、和 Widev CENC ine/。
- 保持規格簡單和可擴展，以支持 future 的DRM系統。
- 使用一個簡單的 RESTAPI.

> **Note**
>
>

主題

- 需要驗證 SPEKE

需要驗證 SPEKE

SPEKE需要內部部署產品以及在AWS雲端中執行的服務和功能的驗證。

主題

AWS雲端實作的驗證

SPEKE需要通過IAM角色進行AWS身份驗證才能與加密器一起使用。IAM角色由DRM提供者或AWS帳戶中擁有DRM端點的操作員建立。每個角色都會指派一個 Amazon 資源名稱 (ARN)，AWSElemental服務操作員在要求加密時會在服務主控台上提供此名稱。必須設定角色的原則權限，才能授與存取金鑰提供者的權限，API而不能存取其他AWS資源。當加密程式聯絡DRM金鑰提供者時，它會使用該角色ARN承擔金鑰提供者帳戶持有者的角色，該角色會傳回用於存取金鑰提供者的加密程式的臨時認證。

一種常見的實作方式是讓操作員或DRM平台廠商在金鑰提供者前面使用 Amazon API Gateway，然後在API閘道資源上啟用 AWS Identity and Access Management (AWSIAM) 授權。您可以使用下列政策定義範例，並將它連接到新的角色，以授予適當資源的許可。在此情況下，權限適用於所有API閘道資源：

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

```
}
```

最後，角色需要新增信任關係，且操作者必須能夠選擇服務。

下列範例顯示為存取DRM金鑰提供者ARN而建立的角色：

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

如需有關建立角色的詳細資訊，請參閱AWS AssumeRole。如需簽署要求的詳細資訊，請參閱AWSSigv4。

內部部署產品的驗證

對於內部部署產品，我們建議您使用SSL/TLS和摘要驗證以獲得最佳安全性，但至少應該使用基本驗證HTTPS。

這兩種類型的身份驗證都使用HTTP請求中的`Authorization`標頭：

- 摘要驗證 — 授權標頭由識別碼`Digest`後跟一系列用於驗證要求的值組成。具體來說，響應值是通過一系列MD5哈希函數生成的，該函數包括來自服務器的唯 one-time-use 一隨機數，用於確保密碼安全地傳輸。
- 基本驗證 — 授權標頭由識別碼組成，`Basic`後面接著代表使用者名稱和密碼的 base-64 編碼字串，並以冒號分隔。

如需有關基本和摘要驗證的資訊，包括標頭的詳細資訊，請參閱網際網路工程工作小組 (IETF) 規格RFC2617-HTTP 驗證：基本和摘要存取驗證。

SPEKEAPIV1

這是RESTAPI用於安全打包器和編碼器密鑰交換（SPEKE）v1。使用此規格為使用加密的客戶提供DRM版權保護。若要SPEKE符合標準，您的DRM金鑰提供者必須公開此規格中RESTAPI所述的內容。加密程式會API呼叫您的金鑰提供者。

> **Note**
>
> 本規定中的代碼範例僅供參考之用。您不能運行這些示例，因為它們不是完整SPEKE實現的一部分。

SPEKE使用DASH產業論壇內容保護資訊交換格式 (DASH-IF-CPIX) 資料結構定義進行金鑰交換，但有一些限制。DASH-IF-CPIX 定義結構描述，以提供從DRM平台到加密器的可擴展多重DRM交換。這可讓系統在內容壓縮和封裝時，能夠對所有自適性位元速率封裝格式進行內容加密。自適應位元速率封裝格式包括HLSDASH、和MSS。

如需有關交換格式的詳細資訊，請參閱DASH產業論壇CPIX規格，網址為 https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf。

主題

SPEKEAPIv1-對 DASH-IF 規範的自定義和約束

DASH如果CPIX規範，https://dashif.org/docs/ DASH-IF-CPIX-v2-0.pdf，支持一些用例和拓撲。該SPEKEAPI規格遵循具有下列自訂和限制的CPIX規格：

- SPEKE 遵循加密程式消費者工作流程。
- 對於加密的內容金鑰，會SPEKE套用下列限制：
  - SPEKE不支援要求或回應承載的數位簽章驗證 (XMLDSIG)。
  - SPEKE需要以 2048 RSA 為基礎的憑證。
- 若要旋轉關鍵工作流程，SPEKE需要`ContentKeyUsageRule`篩選、`KeyPeriodFilter`。SPEKE會忽略所有其他`ContentKeyUsageRule`設定。
- SPEKE 省略 `UpdateHistoryItemList` 功能。如果列表存在於響應中，則SPEKE忽略它。
- SPEKE支援按鍵旋轉。SPEKE僅使用 `ContentKeyPeriod@index 來追蹤金鑰期間。
- 若要支援 MSS PlayReady，請在`DRMSystem`標籤下SPEKE使用自訂參數`SPEKE:ProtectionHeader`。
- 對於HLS封裝，如果回應中存在，則它必須包含要在HLS播放清單`EXT-X-KEY`標籤URI參數中加入的完整資料，而不需要進一步的信號。`URIExtXKey`

- 對於HLS播放清單，在DRMSystem標籤下，SPEKE提供選擇性的自訂參數speke:KeyFormatVersions，speke:KeyFormat並提供EXT-X-KEY標籤KEYFORMAT和KEYFORMATVERSIONS參數的值。

  除非運算符明確指定，否則HLS初始化向量（IV）始終遵循段號。
- 當請求金鑰時，加密程式必須使用 ContentKey 元素上的可選 @explicitIV 屬性。金鑰提供者可以使用 @explicitIV 來回應 IV，即使該屬性未包含在請求中。
- 加密程式會建立金鑰識別符 (KID)，無論任何指定的內容 ID 和金鑰期間都將提供相同識別符。金鑰提供者會在對請求文件的回應中包括 KID。
- 金鑰提供者可能會包含 Speke-User-Agent 回應標頭的值，以自我識別供偵錯之用。
- SPEKE目前不支援每個內容的多個音軌或按鍵。

  SPEKE符合標準的加密器充當客戶端，並將POST操作發送到密鑰提供者端點。加密程式可能會傳送定期的 heartbeat 請求，以確保加密程式與金鑰提供者端點之間的連線情況良好。

SPEKEAPIv1-標準有效載荷組件

在任何SPEKE請求中，加密器可以請求一個或多個DRM系統的響應。加密器指定請求有效負載<cpix:DRMSystemList>的DRM系統。每種系統規格都包括金鑰並指出要傳回的回應類型。

下列範例顯示具有單一DRM系統規格的DRM系統清單：

```
<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>
```

下表列出每個 <cpix:DRMSystem> 的主要元件。

識別符	描述
systemId 或 schemeId	DRM系統類型的唯一識別碼，與 DASH IF 組織一樣。如需清單，請參閱 DASH-IF 系統IDs。

識別符	描述
kid	金鑰 ID。這並非實際金鑰，而是指向雜湊表中的金鑰的識別符。
<cpix:UriExtXKey>	請求標準未加密的金鑰。金鑰回應類型必須是此或 PSSH 回應。
<cpix:PSSH>	要求保護系統特定標頭 (PSSH)。這種類型的標頭包含DRM廠商的kid、、以及自訂資料的參照，做為「通用加密」(CENC) 的一部分。systemID金鑰回應類型必須是此或 UriExtXKey 回應。

_ 標準金鑰與 _ 的請求範例 PSSH

下列範例顯示加密程式向DRM金鑰提供者發出的範例要求的一部分，其中主要元件會反白顯示。第一個請求是一個標準密鑰，而第二個請求是一個PSSH響應：

```
<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>
```

_ 標準金鑰和 _ 的回應範例 PSSH

下列範例顯示DRM金鑰提供者對加密程式的對應回應：

```
<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-即時工作流程方法呼叫範例

請求語法範例

以下URL是一個示例，並不表示固定格式：

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

請求內文

元CPIX素。

請求標頭

名稱	Type	發生	描述
AWS Authorization	字串	1..1	請參閱第AWS四章

名稱	Type	發生	描述
X-Amz-Security-Token	字串	1..1	請參閱第AWS四章
X-Amz-Date	字串	1..1	請參閱第AWS四章
Content-Type	字串	1..1	application/xml

回應標頭

名稱	Type	發生	描述
Speke-User-Agent	字串	1..1	識別金鑰提供者的字串
Content-Type	字串	1..1	application/xml

請求回應

HTTP CODE	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效負載響應
4XX (Client error)	用戶端錯誤訊息	1..1	用戶端錯誤描述
5XX (Server error)	伺服器錯誤訊息	1..1	伺服器錯誤描述

> **Note**
>
> 本節中的範例不包含內容金鑰加密。如需如何新增內容金鑰加密的詳細資訊，請參閱內容金鑰加密。

清除中包含金鑰的即時範例請求承載

下列範例顯示從加密程式傳送至DRM金鑰提供者的典型即時要求承載：

```
<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>
```

清除中包含金鑰的即時範例請求承載

下列範例顯示DRM金鑰提供者的典型回應承載：

```
<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
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEUAUwBDAFQAUgA8AC8AQQ
+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-VOD 工作流程方法調用示例

請求語法範例

以下URL是範例，並不表示固定格式。

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

請求內文

元CPIX素。

回應標頭

名稱	Type	發生	描述
Speke-User-Agent	字串	1..1	識別金鑰提供者的字串
Content-Type	字串	1..1	application/xml

請求回應

HTTP CODE	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效負載響應
4XX (Client error)	用戶端錯誤訊息	1..1	用戶端錯誤描述
5XX (Server error)	伺服器錯誤訊息	1..1	伺服器錯誤描述

> **Note**
>
> 本節中的範例不包含內容金鑰加密。如需有關如何新增內容金鑰加密的詳細資訊，請參閱內容金鑰加密。

VOD使用 Clear 中鍵的示例請求有效負載

下列範例顯示從加密程式傳VOD送至DRM金鑰提供者的基本要求承載：

```
<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>
```

VOD帶有 Clear 鍵的示例響應有效負載

下列範例顯示DRM金鑰提供者的基本VOD回應承載：

```
<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-內容密鑰加密

您可以選擇性地將內容金鑰加密新增至您的SPEKE實作。內容金鑰加密除了加密內容本身之外，還會加密傳輸的內容金鑰，以確保完整的保 end-to-end 護。如果您沒有針對金鑰提供者實作此功能，您必須仰賴傳輸層加密加強式驗證來確保安全性。

若要對在 AWS Cloud 中執行的加密程式使用內容金鑰加密，客戶會將憑AWS證匯入 Certificate Manager，然後將產生的憑證用ARNs於其加密活動。加密程式會使用憑證ARNs和ACM服務，將加密的內容金鑰提供給金鑰提供者。DRM

限制

SPEKE支援 DASH-IF CPIX 規格中指定的內容金鑰加密，但有下列限制：

- SPEKE不支援要求或回應承載的數位簽章驗證 (XMLDSIG)。
- SPEKE需要以 2048 RSA 為基礎的憑證。

這些限制也會列在 [自訂] 和 [DASH-IF 規格的條件約束] 中。

實作內容金鑰加密

若要提供內容金鑰加密，請在金DRM鑰提供者實作中包含下列項目：

- 處理請求和回應承載中的 `<cpix:DeliveryDataList>` 元素。

- 在回應承載的 <cpix:ContentKeyList> 中提供加密值。

如需有關這些元素的詳細資訊，請參閱 DASH-IF CPIX 2.0 規格。

請求承載中的 <cpix:DeliveryDataList> 範例內容金鑰加密元素

下列範例以粗體強調新增的 <cpix:DeliveryDataList> 元素：

```
<?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>
```

回應承載中的 <cpix:DeliveryDataList> 範例內容金鑰加密元素

下列範例以粗體強調新增的 <cpix:DeliveryDataList> 元素：

```
<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>
```

回應承載中的 <cpix:ContentKeyList> 範例內容金鑰加密元素

下列範例說明回應承載 <cpix:ContentKeyList> 元素中的加密內容金鑰處理。其會使用 <pskc:EncryptedValue> 元素：

```
   <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>
```

相比之下，下列範例會顯示類似的回應承載，包含未加密交付的內容金鑰 (做為清除金鑰)。其會使用 <pskc:PlainValue> 元素：

```
    <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-心跳

請求語法範例

以下URL是一個示例，並不表示固定格式：

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

請求回應

HTTP CODE	承載名稱	發生	描述
200 (Success)	statusMessage	1..1	說明狀態的訊息

SPEKEAPIv1-覆蓋密鑰標識符

加密程式會在每次旋轉金鑰時建立新的金鑰識別碼 (KID)。它會在其要求中傳遞KID給DRM金鑰提供者。幾乎總是，密鑰提供者使用相同的響應KID，但它可以為響應KID中的提供不同的值。

以下是具有下列項目的範例要求 KID11111111-1111-1111-1111-111111111111：

```
   <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>
```

下列回應會覆寫KID為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

這是RESTAPI用於安全打包器和編碼器密鑰交換（SPEKE）v2。使用此規格為使用加密的客戶提供DRM版權保護。若要SPEKE符合標準，您的DRM金鑰提供者必須公開此規格中RESTAPI所述的內容。加密程式會API呼叫您的金鑰提供者。

> **Note**
>
> 本規定中的代碼範例僅供參考之用。您不能運行這些示例，因為它們不是完整SPEKE實現的一部分。

SPEKE使用DASH產業論壇內容保護資訊交換格式 (DASH-IF-CPIX) 資料結構定義進行金鑰交換，但有一些限制。DASH-IF-CPIX 定義結構描述，以提供從DRM平台到加密器的可擴展多重DRM交換。這可讓系統在內容壓縮和封裝時，能夠對所有自適性位元速率封裝格式進行內容加密。自適應位元速率封裝格式包括HLSDASH、和MSS。

從它的 2.0 版本開始，SPEKE對齊一個特定的CPIX版本：

在SPEKE側面，這是通過使用X-Speke-VersionHTTP標題來強制執行的，並且通過使用CPIX@version屬性來實施。CPIX請求中缺少這些元素是 SPEKE v1 舊版工作流程的典型情況。在 SPEKE v2 工作流程中，金鑰提供者只有在支援兩個版本參數時才會處理CPIX文件。

有關交換格式的詳細信息，請參閱DASH業界論壇 CPIX2.3 規範。

總體而言，與 1.0 版相比，SPEKEv2.0 帶來了以下進化：SPEKE

- SPEKEXML命名空間中的所有標籤都被棄用，以支持CPIXXML命名空間中的等效標籤
- SPEKE:ProtectionHeader已棄用，並由 CPIX:DRMSystem.SmoothStreamingProtectionHeaderData
- CPIX:URIExtXKey，SPEKE:KeyFormat而且已SPEKE:KeyFormatVersions被棄用，並由 CPIX:DRMSystem.HLSSignalingData
- CPIX@id被取代為 CPIX@contentId
- 新的必要CPIX屬性：CPIX@versionContentKey@commonEncryptionScheme
- 新的可選CPIX元素：DRMSystem.ContentProtectionData
- Support 多個內容金鑰
- 和之間的跨版本控制機制 SPEKE CPIX
- HTTP頭進化：新的X-Speke-Version頭，Speke-User-Agent頭改名為 X-Speke-User-Agent
- 心跳API棄用

由於 SPEKE v1.0 規範保持不變，因此現有的實現不需要更改即可繼續支持 SPEKE v1.0 工作流程。

主題

- SPEKEAPIv2-對 DASH-IF 規範的自定義和約束
- SPEKEAPIv2-標準有效載荷組件
- SPEKEAPIv2-加密合同
- SPEKEAPIv2-實時工作流方法調用示例

- SPEKEAPIv2-VOD 工作流方法調用實例
- SPEKEAPIv2-內容密鑰加密
- SPEKEAPIv2-覆蓋密鑰標識符

SPEKEAPIv2-對 DASH-IF 規範的自定義和約束

DASH產業論壇 CPIX2.3 規格支援多種使用案例和拓撲。SPEKEAPIv2.0 規格定義了CPIX設定檔和用API於CPIX。為了實現這兩個目標，它遵循具有以下自定義和約束的CPIX規範：

CPIX設定檔

- SPEKE 遵循加密程式消費者工作流程。
- 對於加密的內容金鑰，會SPEKE套用下列限制：
  - SPEKE不支援要求或回應承載的數位簽章驗證 (XMLDSIG)。
  - SPEKE需要以 2048 RSA 為基礎的憑證。
- SPEKE僅利用CPIX功能的一部分：
  - SPEKE 省略 `UpdateHistoryItemList` 功能。如果列表存在於響應中，則SPEKE忽略它。
  - SPEKE省略根/葉鍵功能。如果該`ContentKey@dependsOnKey`屬性存在於響應中，則SPEKE忽略它。
  - SPEKE省略元`BitrateFilter`素和`VideoFilter@wcg`屬性。如果這些元素或屬性存在於有CPIX效負載中，請SPEKE忽略它。
- 只有在「標準承載元件」頁面或「加密」合約頁面上參照為「支援」的元素或屬性，才能用於與SPEKE v2 交換的CPIX文件。
- 當加密器包含在CPIX請求中時，所有元素和屬性應在密鑰提供者CPIX響應中攜帶有效值。如果沒有，加密器應停止並拋出錯誤。
- SPEKE支援`KeyPeriodFilter`元素的按鍵旋轉。SPEKE僅使用`ContentKeyPeriod@index`來追蹤金鑰期間。
- 對於HLS信令，必須使用多個`DRMSystem.HLSSignalingData`元素：一個具有「媒體」的`DRMSystem.HLSSignalingData@playlist`屬性值，另一個具有「主」`DRMSystem.HLSSignalingData@playlist` 屬性值。
- 當請求金鑰時，加密程式必須使用 `ContentKey` 元素上的可選 `@explicitIV` 屬性。金鑰提供者可以使用 `@explicitIV` 來回應 IV，即使該屬性未包含在請求中。
- 加密程式會建立金鑰識別符 (`KID`)，無論任何指定的內容 ID 和金鑰期間都將提供相同識別符。金鑰提供者會在對請求文件的回應中包括 `KID`。

- 加密器應包括CPIX@contentId屬性的值。當收到此屬性的空值時，密鑰提供者應返回描述為「缺少 CPIX @contentId」的錯誤。 CPIX@contentId金鑰提供者無法覆寫值。

  CPIX@id值，如果不是 null，則應由密鑰提供者忽略。

- 加密器應包括CPIX@version屬性的值。當收到此屬性的空值時，金鑰提供者應傳回描述為「缺少 CPIX @version」的錯誤。當收到具有不支援版本的要求時，金鑰提供者傳回的錯誤描述應為「不支援的 CPIX @version」。

  CPIX@version金鑰提供者無法覆寫值。

- 加密器應包括每個請求密鑰的ContentKey@commonEncryptionScheme屬性值。當收到此屬性的空值時，密鑰提供者應返回一個錯誤，描述commonEncryptionScheme 為「缺少 ContentKey @ KIDid」。

  唯一CPIX文件無法針對不同ContentKey@commonEncryptionScheme屬性混合使用多個值。當收到這樣的組合時，密鑰提供者應返回一個描述為「不兼容 ContentKey @ commonEncryptionScheme 組合」的錯誤。

  並非所有ContentKey@commonEncryptionScheme值都與所有DRM技術相容。當收到這樣的組合時，密鑰提供者應返回描述 'ContentKey@ 與' commonEncryptionScheme 不兼容 DRMSystem id '的錯誤。

  ContentKey@commonEncryptionScheme金鑰提供者無法覆寫值。

- 當在CPIX響應體中接收到不同的值DRMSystem@PSSH和DRMSystem.ContentProtectionData內部XML<pssh>元素時，加密器應停止並拋出錯誤。

適用於 CPIX 的 API

- 金鑰提供者應包含X-Speke-User-AgentHTTP回應標頭的值。
- SPEKE符合標準的加密器充當客戶端，並將POST操作發送到密鑰提供者端點。
- 加密程序應包括X-Speke-VersionHTTP請求頭的值，與請求一起使用的SPEKE版本，制定為 MajorVersion。 MinorVersion，就像 2.0 版的 SPEKE「2.0」一樣。如果金鑰提供者不支援加密程式針對目前要求所使用的SPEKE版本，金鑰提供者應傳回錯誤，其說明為「不受支援的SPEKE版本」，而不會嘗試以最佳方式處理CPIX文件。

  加密器定義的X-Speke-Version標頭值無法由金鑰提供者在回應要求時修改。

- 在回應主體中收到錯誤時，加密程式應擲回錯誤，而不是使用 SPEKE v1.0 版本重試要求。

如果金鑰提供者沒有傳回錯誤，但無法傳回包含必要資訊的CPIX文件，則加密程式應停止並擲回錯誤。

下表摘要列出訊息主體中金鑰提供者必須傳回的標準訊息。在錯誤的情況下，HTTP響應代碼應該是一個 4XX 或 5XX，從來沒有一個 200。422 錯誤代碼可用於與SPEKE/CPIX相關的所有錯誤。

錯誤大小寫	錯誤訊息
CPIX@ contentId 未定義	遺失 CPIX @ contentId
CPIX@version 尚未定義	遺失 CPIX @version
CPIX不支援 @version	不支援的 CPIX @version
ContentKey@ commonEncryptionScheme 未定義	缺少 ContentKey @ commonEncryptionScheme KIDid（其中id等於 ContentKey @kid 值）
在單個CPIX文檔中使用多個 ContentKey @ commonEncryptionScheme 值	不合規 ContentKey @ commonEncryptionScheme 組合
ContentKey@與commonEncryptionScheme DRM技術不兼容	ContentKey@ commonEncryptionScheme 不兼容 DRMSystemid（其中id等於 DRMSystem @ systemId 值）
X-Speke-版本標頭值不是支援的版本 SPEKE	不支援SPEKE版本
加密合約格式錯誤	格式錯誤的加密合約
加密合同與DRM安全級別限制相矛盾	不支援要求的CPIX加密合約
加密合同不包含任何 VideoFilter 或 AudioFilter 元素	缺少CPIX加密合同

SPEKEAPIv2-標準有效載荷組件

根據針對特定內容定義的加密合約，透過單SPEKE一要求，加密程式可以要求多個內容金鑰，以及針對多種封裝格式所需的 manfest 訊號。

為了涵蓋所有這些方面，標準CPIX文件由三個強制清單區段組成，以及即時內容金鑰旋轉的可選清單區段。

<cpix: ContentKeyList > 區段和最上層<cpix : >元素 CPIX

這是一個強制性部分，與實時和VOD流媒體相關，定義了需要由加密器使用的不同內容密鑰。該<cpix:ContentKeyList>元素可以包含一個或多個<cpix:ContentKey>子元素，每個子元素描述不同的內容鍵。

根據CPIX規範，ContentKey@commonEncryptionScheme屬性的可能值在ISO基礎媒體文件格式文件規範中的通用加密中定義（ISO/IEC23001-7:2016）：

- 'cenc'：AES-CTR 模式完整的樣本和視頻子樣本加密 NAL
- 'cbc1'：AES-CBC 模式完整的樣本和視頻子樣本加密 NAL
- 'cen'：AES-CTR 模式部分視頻NAL模式加密
- 'cbcs'：AES-CBC 模式部分視頻模式加密 NAL

下列範例顯示具有CPIX單一非加密內容金鑰的文件：

```
<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>
```

依預設，內容金鑰不會加密，如以下範例所示。但是加密器可以通過包含<cpix : >元素來請求內容密鑰的加密。DeliveryDataList如需詳細資訊，請參閱內容金鑰加密一節。

支援的元素 SPEKE	必要屬性	選擇性屬性	強制性子元素	可選的子元素
< 個人資料比例：> CPIX	contentId, 版本, XML: CPIX, XML: pskc	名稱，XML: 名稱	一個 <cpix：ContentKeyList>，一個 <cpix：>，一個 <cpix：DRMSystemList> ContentKeyUsageRuleList	一個 <cpix：DeliveryDataList>，一個 <cpix：> ContentKeyPeriodList
< 個人資料比例：> ContentKeyList	-	id	至少有一個 < 個人資料：> ContentKey	-
< 個人資料比例：> ContentKey	孩子 commonEncryptionScheme, 數據	id, 演算法, 明確	一 <pskc:Secret>	-
<pskc:Secret>	PlainValue 或 EncryptedValue	價值 MAC	-	< 選項:EncryptionMethod>, < 一個:> CipherData

< 章節：> 區段 DRMSystemList

這是一個強制性部分，與實時和VOD流媒體相關，定義了需要與內容密鑰一起使用的不同DRM系統。

下列範例顯示具有單一DRM系統規格的 PlayReady DRM系統清單：

```
<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>
```

有關的完整列表 DRMsystemIDs，請參閱 DASH-IF 標識符存儲庫的內容保護部分。

支援的元素 SPEKE	必要屬性	選擇性屬性	強制性子元素	可選的子元素
< 個人資料比例：> DRMSystemList	-	id	至少有一個 < 個人資料：> DRMSystem	-
< 個人資料比例：> DRMSystem	孩子, systemId	身份證，姓名，PSSH	-	ContentProtectionData，SmoothStreamingProtectionHeaderData，兩個 <cpix：HLSSignalingData> 具有不同播放列表屬性值的元素

DRMSystem@PSSH是強制性的，如果 ISO-BMFF 封裝應用於媒體段。DRMSystem.ContentProtectionData內部XML<pssh>元素是由加密僅用於清單信號的目的利用。

如果存DRMSystem@PSSH在並且DRMSystem.ContentProtectionData包含內部XML<pssh>元素，則兩個值應相同。

如果DRMSystem信令是在HLS清單進行，一個<cpix:HLSSignalingData playlist="media">和一個<cpix:HLSSignalingData playlist="master">元素必須包括在CPIX請求和響應。

< 章節：> 區段 ContentKeyPeriodList

這是一個可選部分，僅與實時流媒體相關，定義應用於內容的加密期間。

該<cpix:ContentKeyPeriodList>元素可以包含一個或多個<cpix:ContentKeyPeriod>子元素，每個子元素都描述了實時時間軸中不同的加密時期。使用UUIDs作為 id 屬性值的一部分是一種常用的方法。

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

支援的元素 SPEKE	必要屬性	選擇性屬性	強制性子元素	可選的子元素
< 個人資料比例：> ContentKeyPeriodList	-	id	至少有一個 < 個人資料：> ContentKeyPeriod	-
< 個人資料比例：> ContentKeyPeriod	識別碼，索引	-	-	-

如果使用加密週期，則加密密鑰還需要附加到CPIX文檔中的一個加密期間，如以下部分所示。

< 區段：> 區段 ContentKeyUsageRuleList

這是一個強制性部分，與實時和VOD流媒體相關，定義了不同的內容密鑰如何保護流集內和整個加密期間的曲目。

<cpix: ContentKeyUsageRuleList > 元素可以包含一或多個 <cpix: ContentKeyUsageRule > 子元素，每個元素都描述了加密程序應用給定內容密鑰的軌道，可能在特定的加密期間內。至少有一個 <cpix: AudioFilter > 或一個<cpix : >元素中必須存在一個 <cpix: VideoFilter > 元素中。ContentKeyUsageRule

下列範例顯示一個簡單的清單，其中只有一個規則將單一內容金鑰套用至特定加密期間的所有音訊和視訊軌道。

```
<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>
```

支援的元素 SPEKE	必要屬性	選擇性屬性	強制性子元素	可選的子元素
< 個人資料比例：> ContentKeyUsageRuleList	-	id	至少有一個 < 個人資料：> ContentKeyUsageRule	-
< 個人資料比例：> ContentKeyUsageRule	孩子, intendedTrackType	-	至少有一個 <cpix: AudioFilter > 或一個 <cpix : >(*) VideoFilter	< 個人資料比例：> KeyPeriodFilter
< 個人資料比例：> KeyPeriodFilter	periodId	-	-	-
< 個人資料比例：> AudioFilter	-	minChannels, maxChannels	-	-
< 個人資料比例：> VideoFilter	-	minPixels, 畫maxPixels, 高速公路minFps, maxFps	-	-

(*) 如需使用單一或多個內容金鑰來保護串流集中的一或多個音軌的詳細說明，請參閱加密合約文件一節。 _

SPEKEAPIv2-加密合同

加密合約會根據追蹤特性，定義哪些內容金鑰正在保護指定 Streamset 內的哪些追蹤。

儘管是業界建議的最佳實踐方式，但不是強制性的，但建議您至少使用兩個不同的內容鍵，一個用於音軌，另一個用於視頻軌道。使用單個內容密鑰來加密多個軌道是可能的，但需要在加密器發送給密鑰提供者的CPIX文檔中明確信號。一般而言，加密程式總是會精確描述需要多少個內容金鑰，以及如何利用這些金鑰來加密各種媒體軌道。

原理

加密合同位於CPIX文檔的<cpix:ContentKeyUsageRuleList>部分中。在本節中，在該<cpix:ContentKeyList>部分中定義的每個內容鍵對應於一個特定的<cpix:ContentKeyUsageRule>元素，其中應包括：

- 可參照一個或多個子元件的ContentKeyUsageRule@intendedTrackType屬性，如果使用多個子元件，則以「+」符號分隔。的值ContentKeyUsageRule@intendedTrackType應在加密合同中是唯一的，並且不能在多個ContentKeyUsageRule元素中使用。
- 一個或多個<cpix:AudioFilter>或<cpix:VideoFilter>子元素，這取決於ContentKeyUsageRule@intendedTrackType屬性的值。

管理此關係的規則如下：

- 當流集的所有音頻和視頻軌道都需要使用唯一的內容鍵進行保護時，'ALL'必須使用該字符串作為ContentKeyUsageRule@intendedTrackType屬性值。範例 1 顯示了這樣的使用案例。在這種情況下，a <cpix:AudioFilter /> 和沒有任何屬性的<cpix:VideoFilter />子元素都應包括在內。在此特定上下文中，任何其他<cpix:AudioFilter>和/或<cpix:VideoFilter>元素的組合都是無效的。
- 對於所有其他用例，ContentKeyUsageRule@intendedTrackType屬性的值可以自由定義，並且和<cpix:VideoFilter />子元素的<cpix:AudioFilter />數量必須與通過 '+' 符號聚合的子組件的數量相對應。實例 2/3/4/5/6/7/9/10 說明了這一要求，當一個單一的子組件存在於屬性值。ContentKeyUsageRule@intendedTrackType範例 8 在使用多個子元件時說明它：ContentKeyUsageRule@intendedTrackType="SD+HD"由具有不同屬性值的兩個不同<cpix:VideoFilter>子元素描述，並ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"由具有不同屬性值的三個不同<cpix:VideoFilter>子元素描述。

篩選條件

CPIX定義了多個過濾元素和屬性，但僅SPEKE支持它的一個子集。下表摘要說明這些差異：

CPIX過濾器類型	整體SPEKE支援	支援的篩選器屬性SPEKE	不支援的篩選器屬性SPEKE
< 個人資料比例：> VideoFilter	是	minPixels,maxPixels, hdr,minFps, maxFps (可選屬性)	WCG
< 個人資料比例：> AudioFilter	是	minChannels，maxChannels (選擇性屬性)	
< 個人資料比例：> KeyPeriodFilter	是	periodId （強制屬性）	
< 個人資料比例：> BitrateFilter	否	N/A	N/A
< 個人資料比例：> LabelFilter	否	N/A	N/A

根據的CPIX規格 VideoFilter，[minPixels,maxPixels] 在兩個維度中都是一個全包範圍，而 (minFps,maxFps] 僅適用於尺 maxFps 寸。對於 AudioFilter，[minChannels,maxChannels] 是兩個維度的包含範圍。

問題的情況

在某些情況下，加密合同中提供的信息可能是部分，模糊或錯誤的。在這些情況下，加密程式和金鑰提供者必須採取適當的行為，並確保對內容有適當的保護，這一點很重要。下表顯示在這些情況下建議的行為：

在這種情況下	加密程序應該/應...	金鑰提供者應該/應...
串流集中的一或多個音軌並不適用任何規則 (請參閱下面的範例 3)	加密器應查看其配置（CPIX有效負載外部），並驗證相關軌道不需要加密。如果這不是期望的，加密器應該拋出錯誤並停止處理。	不相關：關鍵提供者不了解流集結構。

在這種情況下	加密程序應該/應...	金鑰提供者應該/應...
多個規則重疊並建議多個內容密鑰來加密特定軌道	加密器應按照文檔的順序應用最後一次 ContentKeyUsageRule 成功評估。	不相關：關鍵提供者不了解流集結構。
加密合約在單SPEKE個請求/響應周期中變化	加密器應引發異常並停止處理，因為密鑰提供商不負責定義加密合同。	為了避免這種情況發生在首位，金鑰提供者不得修改在SPEKE要求的CPIX承載中收到的加密合約。
格式錯誤的加密合同：intendedTrackType/過濾器基數約束異常，不支持的過濾器或屬性	加密程序應引發異常，停止處理，並且不將SPEKE請求發送給密鑰提供商，因為這很可能導致錯誤的內容保護或使某些軌道不受保護。	金鑰提供者應引發例外狀況，並傳回「格式錯誤的加密合約」錯誤。
格式良好的加密合同，但違反了DRM安全級別的約束：例如，要求單個內容密鑰來保護音軌和UHD視頻軌道	如果加密程序已經了解DRM安全級別約束，它應該引發異常，停止處理並且不將SPEKE請求發送給密鑰提供者，因為這很可能會導致錯誤的內容保護。	金鑰提供者應引發例外狀況，並傳回「不支援要求的CPIX加密合約」錯誤。
缺少加密合同	加密器不得發送不包含任何 VideoFilter 或 AudioFilter 元素的CPIX文檔。	金鑰提供者應引發例外狀況，並傳回「缺少CPIX加密合約」錯誤。

加密合約範例

範例 1：適用於所有音訊和視訊軌道的一個內容金鑰

```
<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>
```

範例 2：所有視訊軌道都有一個內容金鑰，所有音軌都有一個內容金鑰

```
<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>
```

範例 3：所有視訊軌道的一個內容金鑰、未加密的音軌

```
<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>
```

範例 4：不同視訊軌道 (SD/HD) 的多個內容金鑰，所有音軌都有一個內容金鑰

```
<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>
```

範例 5：不同視訊軌道 (SD/HD/UHD) 的多個內容鍵，所有音軌都有一個內容金鑰

```
<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>
```

範例 6：不同視訊軌道的多個內容鍵 (SD/HD/UHD1/UHD2)，所有音軌都有一個內容金鑰

```
<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>
```

範例 7：不同視訊軌道的多個內容鍵 (SD/HD1/HD2UHD1/UHD2)，所有音軌都有一個內容金鑰

```
<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>
```

範例 8：不同視訊軌道的多個內容鍵 (根據多種屬性類型)，所有音軌都有一個內容金鑰

```
<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>
```

範例 9：所有視訊軌道都有一個內容按鍵，立體聲和多聲道音軌的多個內容按鍵

```
<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>
```

範例 10：一個內容按鍵可用於所有視訊軌道、多個立體聲內容按鍵，以及兩種多聲道音軌

```
<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-實時工作流方法調用示例

請求語法範例

以下URL是一個示例，並不表示固定格式：

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

請求內文

一CPIX份文件。

請求標頭

名稱	Type	發生	描述
AWS Authorization	字串	1..1	請參閱第AWS四章

名稱	Type	發生	描述
X-Amz-Security-Token	字串	1..1	請參閱第AWS四章
X-Amz-Date	字串	1..1	請參閱第AWS四章
Content-Type	字串	1..1	application/xml
X-Speke-Version	字串	1..1	SPEKEAPI與請求一起使用的版本，制定為 MajorVersion.MinorVersion，就像2.0 版的「2.0」一SPEKE樣

回應標頭

名稱	Type	發生	描述
X-Speke-User-Agent	字串	1..1	識別金鑰提供者的字串
Content-Type	字串	1..1	application/xml
X-Speke-Version	字串	1..1	SPEKEAPI與請求一起使用的版本，制定為 MajorVersion.MinorVersion，就像2.0 版的「2.0」一SPEKE樣

請求回應

HTTP CODE	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效負載響應
4XX (Client error)	用戶端錯誤訊息	1..1	用戶端錯誤描述
5XX (Server error)	伺服器錯誤訊息	1..1	伺服器錯誤描述

> **Note**
>
> 本節中的範例不包含內容金鑰加密。如需有關如何新增內容金鑰加密的資訊，請參閱內容金鑰加密。

清除中包含金鑰的即時範例請求承載

下列範例顯示從加密程式傳送至DRM金鑰提供者的典型即時要求承載，其中包含所有視訊軌道的一個內容金鑰，而所有音訊軌道的一個內容金鑰：

```
<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>
```

清除中包含金鑰的即時範例請求承載

下列範例顯示來自DRM金鑰提供者的典型回應裝載 (傳回值已縮短為 [...]，以提高可讀性)：

```
<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-VOD 工作流方法調用實例

請求語法範例

以下URL是範例，並不表示固定格式。

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

請求內文

一CPIX份文件。

請求標頭

名稱	Type	發生	描述
AWS Authorization	字串	1..1	請參閱第AWS四章
X-Amz-Security-Token	字串	1..1	請參閱第AWS四章
X-Amz-Date	字串	1..1	請參閱第AWS四章
Content-Type	字串	1..1	application/xml
X-Speke-Version	字串	1..1	SPEKEAPI與請求一起使用的版本，制

名稱	Type	發生	描述
			定為 MajorVersion.MinorVersion，就像 2.0 版的「2.0」一SPEKE樣

回應標頭

名稱	Type	發生	描述
X-Speke-User-Agent	字串	1..1	識別金鑰提供者的字串
Content-Type	字串	1..1	application/xml
X-Speke-Version	字串	1..1	SPEKEAPI與請求一起使用的版本，制定為 MajorVersion.MinorVersion，就像 2.0 版的「2.0」一SPEKE樣

請求回應

HTTP CODE	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效負載響應
4XX (Client error)	用戶端錯誤訊息	1..1	用戶端錯誤描述
5XX (Server error)	伺服器錯誤訊息	1..1	伺服器錯誤描述

> **Note**
>
> 本節中的範例不包含內容金鑰加密。如需有關如何新增內容金鑰加密的資訊，請參閱內容金鑰加密。

VOD使用 Clear 中鍵的示例請求有效負載

下列範例顯示從加密程式傳送至DRM金鑰提供者的一般VOD要求承載，其中包含所有視訊軌道的一個內容金鑰，而所有音訊軌道的一個內容金鑰：

```
<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>
```

VOD帶有 Clear 鍵的示例響應有效負載

下列範例顯示來自DRM金鑰提供者的典型回應裝載 (傳回值已縮短為 [...]，以提高可讀性)：

```
<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-內容密鑰加密

您可以選擇性地將內容金鑰加密新增至您的SPEKE實作。內容金鑰加密除了加密內容本身之外，還會加密傳輸的內容金鑰，以確保完整的保 end-to-end 護。如果您沒有針對金鑰提供者實作此功能，您必須仰賴傳輸層加密加強式驗證來確保安全性。

若要對在 AWS Cloud 中執行的加密程式使用內容金鑰加密，客戶會將憑AWS證匯入 Certificate Manager，然後將產生的憑證用ARNs於其加密活動。加密程式會使用憑證ARNs和ACM服務，將加密的內容金鑰提供給金鑰提供者。DRM

限制

SPEKE支援 DASH-IF CPIX 規格中指定的內容金鑰加密，但有下列限制：

- SPEKE不支援要求或回應承載的數位簽章驗證 (XMLDSIG)。
- SPEKE需要以 2048 RSA 為基礎的憑證。

這些限制也會列在 [自訂] 和 [DASH-IF 規格的條件約束] 中。

實作內容金鑰加密

若要提供內容金鑰加密，請在金DRM鑰提供者實作中包含下列項目：

- 處理請求和回應承載中的 <cpix:DeliveryDataList> 元素。
- 在回應承載的 <cpix:ContentKeyList> 中提供加密值。

如需有關這些元素的詳細資訊，請參閱 DASH-IF CPIX 2.3 規格。

請求承載中的 <cpix:DeliveryDataList> 範例內容金鑰加密元素

```
<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>
```

回應承載中的 <cpix:DeliveryDataList> 範例內容金鑰加密元素

```
<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>
```

回應承載中的 <cpix:ContentKeyList> 範例內容金鑰加密元素

下列範例說明回應承載 <cpix:ContentKeyList> 元素中的加密內容金鑰處理。其會使用 <pskc:EncryptedValue> 元素：

```
<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>
```

相比之下，下列範例會顯示類似的回應承載，包含未加密交付的內容金鑰 (做為清除金鑰)。其會使用 <pskc:PlainValue> 元素：

```
<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-覆蓋密鑰標識符

加密程式會在每次旋轉金鑰時建立新的金鑰識別碼 (KID)。它會在其要求中傳遞KID給DRM金鑰提供者。幾乎總是，密鑰提供者使用相同的響應KID，但它可以為響應KID中的提供不同的值。

以下是具有下列項目的範例要求 KID11111111-1111-1111-1111-111111111111：

```
<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>
```

下列回應會覆寫KID為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>
```

SPEKEAPI規格的許可證

創用 CC 姓名標示-ShareAlike 4.0 國際公眾授權條款

通過行使許可權利（定義如下），您接受並同意受本知識共享署名-ShareAlike 4.0 國際公共許可證（以下簡稱「公共許可」）的條款和條件的約束。在本公眾授權得解釋為契約之範圍內，您對該授權條款及條件之同意，為授予您被授權權利之前提，且因授權人自依據條款及條件提供被授權資料所受利益，授權人授予您前開權利。

第 1 條 – 定義

a. 改編素材指自授權素材所衍生，其經以授權人主張之著作權或其相似權利許可方式所為之翻譯、改變、編排、轉化或其他變更方式，而受到著作權及其相似權利保護之素材。基於本公眾授權目的，當授權素材為音樂著作、表演或聲音錄製，改編素材依據時間序列與動態影像同步化 (下稱「同步化」)。

b. 轉接器的許可證是指您根據本公共許可證的條款和條件對改編材料的貢獻中適用於您的著作權和類似權利的許可。

c. BY-SA 兼容許可證是指在創意共享許可證中列出的許可證，由創用共享許可證批准為本公共許可證實際上等同於本公共許可證。

d. 著作權及其相似權利係指著作權及/或其與著作權密切相關之相似權利，包括但不限於演播、廣播、聲音錄製及資料庫特有權利，且無須考慮權利之標示或分類。基於本公眾授權之目的，第 2 條第 (b) 項 第(1) 至 (2) 款指名之權利並非著作權及其相似權利。

e. 有效的技術措施是指在沒有適當權限的情況下，根據 1996 年 12 月 20 日通過的《WIPO版權條約》第 11 條和/或類似國際協議中履行義務的法律規避的措施。

f. 除外及限制條款係指合理使用、合理處理且/或其他適用於您使用授權素材之著作權或其相似權利所為除外或限制規定。

g. 「授權元素」是指以創用 CC 公共授權條款名稱列出的授權屬性。本公眾授權條款的授權要素為姓名標示和 ShareAlike。

h. 授權素材係指藝術或文學創作、資料庫或其他授權人對其適用公眾授權之素材。

i. 授權權利係指依據本公眾授權之條款及條件授予給您之權利，其限於所有您授權素材之使用所適用之著作權及其相似權利，以及授權人有權授權者。

j. 授權人係指依據本公眾授權授予權利之個人或實體。

k. 分享係指透過任何需要取得授權權利允許之方式或程序提供素材予公眾，例如重製、公開展示、公開表演、散佈、宣傳、通訊或進口，並使公眾得以取得素材，包括使公眾得從其各自選定之地點存取素材之方式。

l. 資料庫特有權利係指，除著作權外，其他依據歐洲議會及理事會 1996 年 3 月 11 日第 96/9/EC 號「歐體資料庫法律保護指令」(包含該指令的任何修改或後續版) 有關資料庫法定保護所生之權利，及全球各地其他本質相同之權利。

m.「您」係指依據本公眾授權行使權利之個人或實體。「您的」亦有一相對應之定義。

第 2 條 - 範圍。

a. 授權同意。

1. 依據本公眾授權之條款及條件，授權人於此授予您免權利金、不得轉授權、非專屬性、不可撤回的授權，以於授權素材中行使授權權利：

   A. 複製及分享授權素材的全部或部分；以及

   B. 產生、重製和分享改用素材。

2. 除外及限制規定。為避免疑義，當除外及限制規定適用於您的使用，本公眾授權即不適用，且您無須遵守本公眾協議之條款及條件。

3. 條款。公眾授權條款規定於第 6 條第 (a) 項規定。

4. 允許媒介及形式以及技術修改。授權人授權您於所有媒介及形式上行使授權權利，無論其為現行已知或其後所發明創作者，並可為必要之技術修改。授權人拋棄且/或同意不主張以任何權利或權力，禁止您為行使本授權權利所做之必要技術修改，包括以必要技術修改以規避有效技術措施。基於本公眾授權之目的，僅依據第 2 條第 (a) 項第 (4) 款所授權之修改，並不會因此製造出改作素材。

5. 後續接受者。

   A. 授權人所提供條件 - 授權素材。每一授權素材之接受者自動取得授權人所提供依據本公眾授權條款及條件行使授權權利之條件。

   B. 授權人提供的其他優惠 — 改編材料。根據您所申請的轉接器授權條件，您的每位改用材料接收者都會自動收到授權人提出的要約，以行使改用材料中的授權權利。

   C. 無後續限制。您不得對授權素材提供任何額外或不同之條款或條件，或是用有效科技措施於授權素材，倘前開情形將限制授權素材接受者之授權權利行使。

6. 無背書。本公眾協議並未構成且不得解釋為以下情況：同意您主張或暗示，您或您授權素材之使用與第 3 條第 (a) 項第 (1) 款 第(A) (i) 目規定表彰之授權人或其指定之人有關聯，或受該授權人或其指定之人贊助、背書或授予正式地位。

b. 其他權利。

1. 著作人格權 (例如完整性保持權) 既未據本公眾授權條款授權，也非屬公眾、隱私或其他相似人格權，惟授權人在允許您行使授權權利 (而非其他權利) 所需之範圍內，盡可能拋棄及/或同意不主張其所有之任何前開權利。

2. 專利權及商標權並未依據本公眾授權協議授權。

3. 授權人盡可能拋棄向您收取行使授權權利相關權利金之權利，無論是否直接或透過基於自願性或可免除法定或強制性授權機制之權利金代收團體收取。在所有其他情形，授權人明確保留收取權利金之任何權利。

第 3 條 – 授權條件。

您行使授權權利明確受到下列條件規範。

a. 姓名標示。

1. 倘您分享授權素材 (包括以修改形式所為)，您必須：

   A. 如果授權人提供授權材料，則保留以下內容：

```
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. 指出您是否修改了授權材料，並保留任何先前修改的指示；以及

   C. 表示授權材料是根據本公眾授權條款授權，並包含本公眾授權條款的文字URI或超連結。

2. 在您分享授權素材之媒介、方式或環境下，您得以任何適當方式滿足第3 條第 (a) 項第 (1) 款之條件。例如，透過提供URI或超連結至包含所需資訊的資源，以滿足條件可能是合理的。

3. 倘經授權人請求，您須於適切可行之範圍內，移除第 3 條第 (a) 項第 (1) 款第 (A) 目所規定之資訊。

b. ShareAlike。除了第 3 (a) 條中的條件外，如果您分享您生產的改用材料，則下列條件也適用。

1. 您申請的適配器許可必須是具有相同許可元素的創用 CC 許可，此版本或更高版本，或 BY-SA 兼容許可證。

2. 您必須包含您所申請之轉接器授權的文字URI或超連結。您可以根據您分享改用素材的媒介、方式和背景，以任何合理的方式滿足此條件。

3. 您不得對「改用材料」提供或施加任何額外或不同的條款或條件，或對「改用材料」套用任何有效的技術措施，以限制您所適用的轉接器授權所授予的權利的行使。

第 4 條 – 資料庫特有權利。

當授權權利包括您使用授權素材所適用之資料庫特有權利：

a. 為避免疑義，第 2 (a) (1) 條授予您擷取、再利用、複製及分享資料庫內容的全部或相當部分的權利；

b. 如果您在您擁有 Sui Generis 資料庫權利的資料庫中包含全部或大部分資料庫內容，則您擁有 Sui Generis 資料庫權利的資料庫 (但不包括其個別內容) 的資料庫為改編材料，包括用於第 3 (b) 條；以及

c. 倘您分享該資料庫全部或重要部分之內容，您必須遵守第 3 條第 (a) 項規定之條件。為避免疑義，若授權權利包括著作權及其相似權利，則第 4 條係補充而非取代您依據本公眾授權協議義務之規定。

第 5 條 – 免除保證聲明及責任限制。

a. 除授權人另有個別承諾，授權人應於可能範圍內以「現狀」及「現時可得」提供授權素材，且不論明示、暗示、或無論法律有無規定，均無關於授權素材之任何聲明或保證。此包括但不限有關權利擔保、適售性、特定目的適用性、無侵權、不具潛在或其他缺陷、正確性，或不具備無論是否已知或能否被發現的錯誤。當法律不允許全部或部分免除保證責任，則此免責聲明可能對您不適用。

b. 在可能範圍內，對於任何因本公眾授權或授權素材使用致生直接、特殊、間接、衍生、懲罰性或警告性損害，或其他損失、費用、支出或其他損害，授權人在法理上對您不負任何責任。縱使授權人已被告知發生此類損失、費用、支出或損害的可能性時，亦同。若法律不允許全部或一部之責任限制，則此限制規定可能對您並不適用。

c. 上開規定之免除保證聲明及責任限制應盡可能以完全免責或責任拋棄之方式加以解釋。

第 6 條 – 期間與終止。

a. 本公眾授權條款於著作權及其相似權利授權之期間範圍內適用。但若您未能遵守本公眾授權協議，您依據本公眾授權協議所取得之權利將自動終止。

b. 當您使用授權素材之權利業已依據第 6 條第 (a) 項終止，其應於下列情形恢復效力：

   1. 自違規治愈之日起自動，前提是在您發現違規行為後 30 天內治愈；或

   2. 經授權人明示復原。

c. 為免疑義，第 6 條第 (b) 項並未影響任何授權人因您違反本公眾授權協議而得以請求救濟措施之權利。

d. 為免疑義，授權人亦得依據不同的條款或條件提供授權素材，或於任何時點停止散佈授權素材，但前開行為並不會終止本公眾授權。

e. 本公眾授權協議之終止對於第 1、5、6、7 條及第 8 條之效力不生影響。

第 7 條 – 其他條款及條件。

a. 除明示同意者外，授權人不受到您所傳達任何額外或不同條款或條件之拘束。

b. 任何本協議未規定之任何授權素材相關安排、諒解或約定，均不屬於與本公眾授權條款及條件，且獨立存在。

第 8 條 - 條文解釋。

a. 為了避免疑義，對於無須依據本公眾授權協議許可即可合法使用之授權素材，本公眾授權並未且不得被解釋為削弱、限制其使用或對使用附加條件。

b. 倘本公眾授權任何條款被視為無法強制執行，其應在使其具有執行力所需範圍內自動修訂為可以執行。倘該條款無法修訂，其應與本公眾授權協議切割，且不影響其他條款及條件之可執行性。

c. 除經授權人明示同意，本公眾授權條款或條件不得免除，且不得同意授權條款或條件之違反。

d. 本公眾授權並未構成，亦不得解釋為限制或拋棄任何適用於授權人或您之特權或豁免，包括任何司法管轄區或有權機關法律程序所生之特權或豁免。

SPEKE 合作夥伴和客戶指南的文件歷史記錄

下表說明SPEKE文件的變更。

SPEKE v1

變更	描述	日期
支援矩陣：AWS合作夥伴服務和產品	新增了AWS合作夥伴服務和產品SPEKE支援的新區段，列出 Bitmovin 服務。	2023 年 1 月 13 日
DRM 平台供應商的更新	已將連結和新的合作夥伴資訊新增至DRM平台提供者清單。	2019 年 1 月 24 日
包括第三方加密程式	更新架構和描述，以說明第三方加密程式。	2018 年 11 月 20 日
內容金鑰加密	新增加密內容金鑰的選項。在此之前，Secure Packager 和 Encoder Key Exchange 僅支援透明金鑰交付。	2018 年 10 月 30 日
支援矩陣 - AWS Elemental Live	新增了 AWS Elemental Live 支援矩陣。	2018 年 9 月 27 日
標準承載元件	新增了定義JSON承載中主要元素的區段。	2018 年 9 月 27 日
KID 覆寫	已新增金鑰提供者KID覆寫的相關區段。	2018 年 9 月 27 日
更正 DASH-IF 網站的連結	更正 IF DASH 網站的連結，以取得CPIX規格和系統IDs頁面。	2018 年 9 月 27 日
AWS Elemental Live 的版本複本	更新SPEKE文件以包含 AWS Elemental 產品。	2018 年 7 月 20 日

變更	描述	日期
CMAF	更新 服務的支援資料表，以包含通用媒體應用程式格式（CMAF）。	2018 年 6 月 27 日
初始版本	Secure Packager 和 Encoder Key Exchange（SPEKE）第 1 版的初始版本，這是內容加密器與DRM金鑰提供者之間通訊的規格。DRM 金鑰提供者公開 Secure Packager 和 Encoder Key Exchange API來處理傳入的金鑰請求。	2017 年 11 月 27 日

SPEKE v2

變更	描述	日期
DRM 平台提供者區段的更新，以及 AWS服務和產品支援SPEKE區段	已將 Webstream 新增至DRM平台提供者清單的 SPEKE v2 欄， MediaConvert 並新增至AWS服務和產品資料表中SPEKE支援的 SPEKE v2 欄。	2024 年 10 月 10 日
DRM 平台提供者的更新區段	已將新的合格合作夥伴新增至DRM平台提供者清單的 SPEKE v2 欄。	2023 年 8 月 9 日
即時和VOD工作流程方法呼叫範例區段的更新	在 SPEKE v2 Live 和VOD工作流程方法呼叫範例區段中新增缺少 X-Speke-Version的回應標頭。	2023 年 1 月 13 日
DRM 平台提供者和加密合約區段的更新	已將新的合格合作夥伴新增至DRM平台提供者清單的 SPEKE v2 欄。新增了兩個加密合約的新範例，並在所有相	2022 年 1 月 27 日

變更	描述	日期
	關範例中將 SD 最大解析度變更為 1024x576。	
初始版本	Secure Packager 和 Encoder Key Exchange（SPEKE）2.0 版的初始版本，這是內容加密器與DRM金鑰提供者之間通訊的規格。DRM 金鑰提供者公開 Secure Packager 和 Encoder Key Exchange API來處理傳入的金鑰請求。	2021 年 9 月 7 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。