合作夥伴和客戶指南

Secure Packager 和 Encoder Key Exchange API 規格

Secure Packager 和 Encoder Key Exchange API 規格: 合作夥伴和客戶指南

Table of Contents

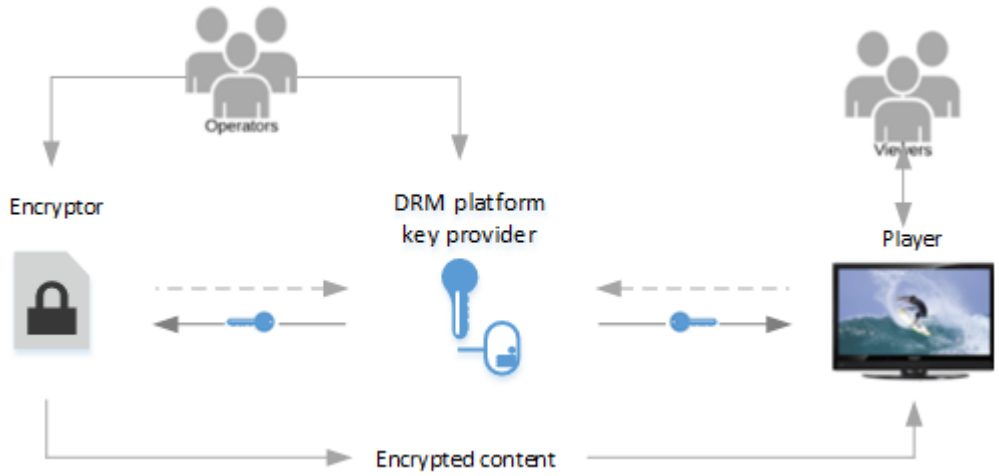
什麼是安全封裝程式和編碼器金鑰交換？

安全封裝程式和編碼器金鑰交換 (SPEKE) 定義了媒體內容加密程式和封裝程式與數位權利管理 (DRM) 金鑰提供者之間的通訊標準。此規格適用於在內部部署和 AWS 雲端中執行的加密程式。

主題

一般架構

下圖顯示現場部署產品的 SPEKE 內容加密架構的高階檢視。

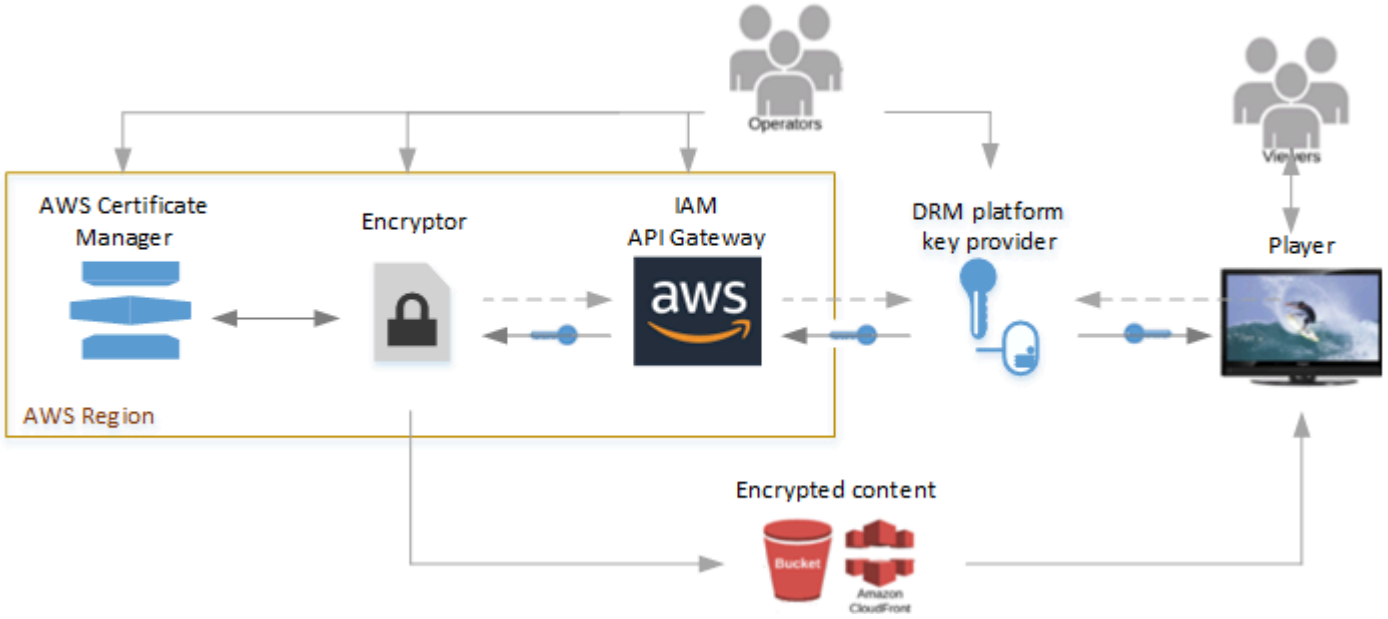


這些是上述架構的主要元素：

- Encryptor – 提供加密技術。接收來自操作者的加密請求，並從 DRM 金鑰提供者擷取所需金鑰，以保護加密的內容。
- DRM 平台金鑰提供者 – 透過 SPEKE 相容 API 提供加密金鑰給加密器。提供者也為媒體播放器提供解密授權。
- 播放器 – 請求來自相同 DRM 平台金鑰提供者的金鑰，播放器會用來解鎖內容並將其提供給檢視者。

AWS 雲端架構

下圖顯示將 SPEKE 與在 AWS 雲端中執行的服務和功能搭配使用時的概要架構。



這些是主要服務和元件：

- Encryptor – 在 AWS 雲端中提供加密技術。加密程式接收來自操作者的請求，並透過 Amazon API Gateway 從 DRM 金鑰提供者擷取所需加密金鑰，以保護加密的內容。系統會將加密的內容交付給 Amazon S3 儲存貯體，或透過 Amazon CloudFront 散發。
- AWS IAM 和 Amazon API Gateway – 管理加密程式和金鑰提供者之間的客戶信任角色和代理通訊。API Gateway 提供記錄功能，讓客戶控制其與加密程式和 DRM 平台之間的關係。客戶可透過 IAM 角色組態啟用金鑰提供者存取。API Gateway 必須位於與加密程式相同的 AWS 區域。
- AWS Certificate Manager –（選用）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。Certificate Manager 所在的 AWS 區域必須與加密程式相同。
- DRM 平台金鑰提供者 – 透過 SPEKE 相容 API 提供加密金鑰給加密器。提供者也為媒體播放器提供解密授權。
- 玩家 – 從相同的 DRM 平台金鑰提供者請求金鑰，該提供者會用來解鎖內容並將其提供給檢視者。

如何開始

如需 SPEKE 的其他簡介資料，請參閱您是初次使用 SPEKE 嗎？

您是客戶嗎？

與 AWS Elemental DRM 平台供應商建立合作夥伴關係，以取得設定使用加密。如需詳細資訊，請參閱客戶加入。

您是 DRM 平台供應商，還是自有金鑰提供者的客戶？

根據 SPEKE 規格公開金鑰提供者的 REST API。如需詳細資訊，請參閱 SPEKE API 規格。

您是第一次使用 SPEKE 嗎？

本節為初次使用 Secure Packager 和 Encoder Key Exchange (SPEKE) 的讀者提供簡介資訊。

如需 SPEKE 簡介，請觀看下列網路廣播：

相關服務資訊和規格

- API 閘道許可 – 如何使用 AWS Identity and Access Management (AWS IAM) 許可控制對 API 的存取。
- AWS AssumeRole – 如何使用 AWS Security Token Service (AWS STS) 擔任角色功能。
- AWS Sigv4 – 如何使用 Signature 第 4 版簽署 HTTP 請求。
- DASH-IF CPIX 規格 v2.0 – DASH-IF 內容保護資訊交換格式 (CPIX) 規格版本，此 SPEKE v1.0 規格是以其為基礎。
- DASH-IF CPIX 規格 v2.3 – DASH-IF 內容保護資訊交換格式 (CPIX) 規格版本，此 SPEKE v2.0 規格是以其為基礎。
- DASH-IF IDs – DRM 系統的註冊識別符清單。
- https://github.com/awslabs/speke-reference-server：// – 要與您的 AWS 帳戶搭配使用的參考金鑰提供者範例，可協助您在 AWS 中開始使用 SPEKE 實作。

術語

下列清單定義此規定中使用的術語。此規定盡可能遵循在 DASH-IF CPIX 規定 中使用的術語。

- ARN – Amazon Resource Name。唯一識別 AWS 資源。
- 內容金鑰 – 用於加密部分內容的密碼編譯金鑰。
- 內容提供者 – 提供交付受保護媒體之權利和規則的發佈者。內容供應商可能也提供來源媒體 (用於轉碼的 Mezzanine 格式)、資產識別符、金鑰識別符 (KID)、索引鍵值、編碼指示，以及內容描述中繼資料。
- DRM – 數位權利管理。用於防止版權數位內容未經授權的存取。
- DRM 平台 – 為內容加密者和檢視器提供 DRM 功能和支援的系統，包括提供 DRM 金鑰和內容加密和解密的授權。
- DRM 提供者 – 請參閱 DRM 平台。

- DRM 系統 – DRM 實作的標準。常見的 DRM 系統包括 Apple FairPlay、Google Widevine 和 Microsoft PlayReady。內容供應商使用 DRM 系統來保護數位內容，以傳輸給檢視者或由檢視者存取。如需已向 DASH-IF 註冊的 DRM 系統清單，請參閱 DASH-IF 系統 IDs。DASH-IF CPIX 規定 使用如本文定義的「DRM 系統」，且在某些地方，它會使用「DRM 系統」表示此規定是指 DRM 平台。
- DRM 解決方案 – 請參閱 DRM 平台。
- DRM 技術 – 請參閱 DRM 系統。
- 加密程式 – 媒體處理元件，使用從金鑰提供者取得的金鑰來加密媒體內容。加密程式一般也會將 DRM 加密訊號和中繼資料新增至媒體。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，公開 SPEKE REST API 來處理金鑰請求。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 – DRM 平台的元件，可維護內容加密和解密的金鑰。
- 操作員 – 負責操作整體系統的人員，包括加密程式和金鑰提供者。
- 播放器 – 代表檢視器操作的媒體播放器。取得來自不同來源的資訊，包括媒體資訊清單檔案、媒體檔案和 DRM 授權。代檢視者請求來自 DRM 平台的授權。

SPEKE 的客戶加入

將 Secure Packager and Encoder Key Exchange (SPEKE) 數位版權管理 (DRM) 金鑰提供者與您的加密程式和媒體播放器結合，保護您的內容不受未經授權的使用。SPEKE 定義了媒體內容加密程式和封裝程式與數位版權管理 (DRM) 金鑰提供者之間的通訊標準。若要入門，您可以選擇 DRM 平台金鑰供應商，並設定金鑰供應商與加密程式和播放器之間的通訊。

主題

開始使用 DRM 平台供應商

下列 Amazon 合作夥伴提供適用於 SPEKE 的第三方 DRM 平台實作。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 合作夥伴網路頁面，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 平台提供者	SPEKE v1 支援	SPEKE v2 支援
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
DOVERUNNER	√	√
Insys 雲端 DRM	√	√
Intertrust Technologies	√	√
Irdeto	√	√

DRM 平台提供者	SPEKE v1 支援	SPEKE v2 支援
JW 播放器	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

AWS 服務和產品的 SPEKE 支援

本節列出在 AWS 雲端中執行的 AWS 媒體服務與 AWS 現場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程式。確認您所需的串流通訊協定和 DRM 系統是否適用於您的服務或產品。

AWS 服務或產品	SPEKE v1 支援	SPEKE v2 支援	支援的 DRM 技術
AWS Elemental MediaConvert - 在 AWS 雲端中執行的服務	√	√	文件
AWS Elemental MediaPackage - 在 AWS 雲端中執行的服務	√	√	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	支援的 DRM 技術
AWS Elemental Server - 內部部署產品	√		文件

AWS 合作夥伴服務和產品的 SPEKE 支援

本節列出 AWS 合作夥伴服務和在 AWS 雲端中執行的產品所提供的 SPEKE 支援。這些服務和產品是 SPEKE 內容加密架構中的加密程式。確認您所需的串流通訊協定和 DRM 系統是否適用於您的服務或產品。

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

SPEKE API 規格

這是 Secure Packager and Encoder Key Exchange (SPEKE) 的 REST API 規格。使用此規格為使用加密的客戶提供 DRM 版權保護。

在影片串流工作流程中，加密引擎會與 DRM 平台金鑰提供者通訊，以請求內容金鑰。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，以實現更安全的端對端加密。

此規定旨在達成下列目標：

- 定義簡單、可信任、高度安全的介面，讓 DRM 廠商和客戶可在需要加密內容時，使用該介面來整合加密程式。
- 涵蓋 VOD 和即時工作流程，並包括在加密程式與 DRM 金鑰提供者端點之間進行強大、高度安全的通訊時所需的錯誤情況和身分驗證機制。
- 包括支援 HLS、MSS 和 DASH 封裝及其常見的 DRM 系統：FairPlay、PlayReady 和 Widevine/CENC。
- 保持規定簡單且可擴展，以支援未來的 DRM 系統。
- 使用簡易的 REST API。

> **Note**
>
>

主題

SPEKE 所需的身分驗證

SPEKE 需要現場部署產品的身分驗證，以及在 AWS 雲端中執行的服務和功能。

主題

AWS 雲端實作的身分驗證

SPEKE 需要透過 IAM 角色進行 AWS 身分驗證，才能與加密器搭配使用。IAM 角色由 DRM 提供者或在 AWS 帳戶中擁有 DRM 端點的操作者建立。系統會將 Amazon Resource Name (ARN) 指派給每個角色，AWS Elemental 服務操作者會在請求加密時，在服務主控台上提供該名稱。必須設定角色的政策許可，以授予存取金鑰提供者 API 的許可，並且不允許其他 AWS 資源存取。當加密程式聯絡 DRM 金鑰提供者時，它會使用角色 ARN 來擔任金鑰提供者帳戶持有人的角色，系統會傳回臨時憑證以供加密程式用於存取金鑰提供者。

其中一個常見實作是讓運算子或 DRM 平台供應商在金鑰提供者前面使用 Amazon API Gateway，然後在 API Gateway 資源上啟用 AWS Identity and Access Management (AWS IAM) 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， 許可適用於所有 API Gateway 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。

下列範例說明建立用於存取 DRM 金鑰提供者的角色 ARN：

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

如需建立角色的詳細資訊，請參閱 AWS AssumeRole。如需簽署請求的詳細資訊，請參閱 AWS Sigv4。

現場部署產品的身分驗證

對於現場部署產品，我們建議您使用 SSL/TLS 和摘要身分驗證以獲得最佳安全性，但至少應使用透過 HTTPS 的基本身分驗證。

兩種類型的身分驗證都會在 HTTP 請求中使用 `Authorization` 標頭：

- 摘要身分驗證 – 授權標頭包含識別符`Digest`，後面接著一系列驗證請求的值。具體來說，系統會透過一系列 MD5 雜湊函數產生回應值，這些函數包括來自伺服器的唯一一次性使用的 nonce，用於確保密碼安全傳輸。
- 基本身分驗證 – 授權標頭包含識別符`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。

如需基本和摘要驗證的資訊，其中包括標頭的詳細資訊，請參閱 Internet Engineering Task Force (IETF) 規定 RFC 2617 - HTTP 身分驗證：基本和摘要存取驗證。

SPEKE API v1

這是 REST API for Secure Packager and Encoder Key Exchange (SPEKE) v1。使用此規格為使用加密的客戶提供 DRM 版權保護。若要符合 SPEKE，您的 DRM 金鑰提供者必須公開本規格中所述的 REST API。加密程式會對您的金鑰提供者進行 API 呼叫。

> **Note**
>
> 本規定中的代碼範例僅供參考之用。您無法執行這些範例，由於它們不是完整 SPEKE 實作的一部分。

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 會定義結構描述，以提供從 DRM 平台到加密程式的可擴展、多 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。自適性位元速率封裝格式包括 HLS、DASH 和 MSS。

如需交換格式的詳細資訊，請參閱位於 https：//https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf 的 DASH 產業論壇 CPIX 規格。

主題

SPEKE API v1 - DASH-IF 規格的自訂和限制

DASH-IF CPIX 規格 https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf：//。SPEKE API 規格遵循 CPIX 規格，具有下列自訂和限制條件：

- SPEKE 遵循 Encryptor Consumer 工作流程。
- 對於加密的內容金鑰，SPEKE 會套用下列限制：
  - SPEKE 不支援請求或回應承載的數位簽章驗證 (XMLDSIG)。
  - SPEKE 需要 2048 RSA 型憑證。
- 對於輪換金鑰工作流程，SPEKE 需要`ContentKeyUsageRule`篩選條件 `KeyPeriodFilter`。SPEKE 會忽略所有其他`ContentKeyUsageRule`設定。
- SPEKE 會省略 `UpdateHistoryItemList`功能。如果回應中有清單，SPEKE 會忽略清單。
- SPEKE 支援金鑰輪換。SPEKE 僅使用 `ContentKeyPeriod@index 來追蹤金鑰期間。
- 為了支援 MSS PlayReady，SPEKE 會在`DRMSystem`標籤 下使用自訂參數`SPEKE:ProtectionHeader`。
- 對於 HLS 封裝，如果 `URIExtXKey` 出現在回應中，則其必須包含要新增到 HLS 播放清單 `EXT-X-KEY` 標籤 URI 參數中的完整資料，而無需進一步訊號要求。
- 對於 HLS 播放清單，在`DRMSystem`標籤下，SPEKE 會提供選用的自訂參數 `speke:KeyFormat`和 `speke:KeyFormatVersions`，用於`EXT-X-KEY`標籤的 `KEYFORMAT`和 `KEYFORMATVERSIONS` 參數值。

  除非操作者明確指定，否則 HLS 初始向量 (IV) 會一律遵循區段號碼。

- 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索引鍵。

  符合 SPEKE 的加密程式會做為用戶端，並將POST操作傳送至金鑰提供者端點。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。

SPEKE API v1 - 標準承載元件

在任何 SPEKE 請求中，加密程式可以請求一或多個 DRM 系統的回應。加密程式會在請求承載的 <cpix:DRMSystemList> 中指定 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 DRM 系統清單與單一 DRM 系統規定：

```
<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符，已向 DASH IF 組織註冊。如需清單，請參閱 DASH-IF 系統 ID。
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。

識別符	描述
<cpix:PSSH>	要求保護系統特定標頭 (PSSH)。這類標頭包含 kid 和 systemID 的參考，以及 DRM 廠商的自訂資料，作為一般加密 (CENC) 的一部分。金鑰回應類型必須是此或 UriExtXKey 回應。

_標準金鑰和 PSSH _ 的請求範例

下列範例會顯示從加密程式到 DRM 金鑰提供者的一部分範例請求，並詳加說明主要元件。第一種請求適用於標準金鑰，第二個請求則適用於 PSSH 回應：

```
<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 PSSH _ 的回應範例

下列範例顯示從 DRM 金鑰提供者到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>
```

SPEKE API v1 - 即時工作流程方法呼叫範例

請求語法範例

下列 URL 範例僅供參考，格式並非固定不變：

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

請求內文

CPIX 元素。

請求標頭

名稱	Type	發生	描述
`AWS Authorization`	字串	1..1	請參閱 AWS Sigv4

名稱	Type	發生	描述
X-Amz-Security-Token	字串	1..1	請參閱 AWS Sigv4
X-Amz-Date	字串	1..1	請參閱 AWS Sigv4
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 代碼	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 承載回應
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

下列範例說明從加密程式到 DRM 金鑰提供者的典型即時請求承載：

```
<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

下列範例說明來自 DRM 金鑰供應商的典型回應承載：

```
<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
+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>
```

SPEKE API v1 - VOD 工作流程方法呼叫範例

請求語法範例

下列 URL 範例僅供參考，格式並非固定不變。

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

請求內文

CPIX 元素。

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 代碼	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 承載回應
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資訊，請參閱內容金鑰加密。

清除中包含金鑰的 VOD 範例請求承載

下列範例說明從加密程式到 DRM 金鑰提供者的基本 VOD 請求承載：

```
<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>
```

清除中包含金鑰的 VOD 範例請求承載

下列範例說明來自 DRM 金鑰供應商的基本 VOD 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>
```

SPEKE API v1 - 內容金鑰加密

您可以選擇將內容金鑰加密新增至 SPEKE 實作。除了加密內容本身外，內容金鑰加密還會透過加密內容金鑰進行傳輸，以確保完整的端對端保護。如果您未為金鑰提供者實作此項目，則需依賴傳輸層加密加上強式身分驗證以確保安全。

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

限制

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

- SPEKE 不支援請求或回應承載的數位簽章驗證 (XMLDSIG)。
- SPEKE 需要 2048 RSA 型憑證。

這些限制也會列在自訂和 DASH-IF 規格的限制中。

實作內容金鑰加密

若要提供內容金鑰加密，請在您的 DRM 金鑰提供者實作中包含下列內容：

- 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。

如需這類元素的詳細資訊，請參閱 DASH-IF CPIX 2.0 規定。

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>
```

SPEKE API v1 - 心跳

請求語法範例

下列 URL 範例僅供參考，格式並非固定不變：

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

請求回應

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

SPEKE API v1 - 覆寫金鑰識別符

加密程式會在每次輪換金鑰時建立新的金鑰識別符 (KID)。它會在請求中將 KID 傳遞到 DRM 金鑰提供者。金鑰提供者通常會使用相同的 KID 進行回應，但它可以為回應中的 KID 提供不同的值。

下列是 KID 的範例請求 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>
```

下列回應會將 KID 覆寫為 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>
```

SPEKE API v2

這是 REST API for Secure Packager and Encoder Key Exchange (SPEKE) v2。使用此規格為使用加密的客戶提供 DRM 版權保護。若要符合 SPEKE，您的 DRM 金鑰提供者必須公開本規格中所述的 REST API。加密程式會對您的金鑰提供者進行 API 呼叫。

> **Note**
>
> 本規定中的代碼範例僅供參考之用。您無法執行這些範例，由於它們不是完整 SPEKE 實作的一部分。

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 會定義結構描述，以提供從 DRM 平台到加密程式的可擴展、多 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。自適性位元速率封裝格式包括 HLS、DASH 和 MSS。

從其 2.0 版開始，SPEKE 會與特定 CPIX 版本一致：

在 SPEKE 端，這是透過使用 `X-Speke-Version` HTTP 標頭，以及在 CPIX 端透過使用 `CPIX@version` 屬性強制執行。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，只有在金鑰提供者同時支援兩個版本參數時，才會預期其會處理 CPIX 文件。

如需交換格式的詳細資訊，請參閱 DASH 產業論壇 CPIX 2.3 規格。

整體而言，相較於 SPEKE 1.0 版，SPEKE 2.0 版帶來了以下演變：

- 來自 SPEKE XML 命名空間的所有標籤都會取代，以有利於 CPIX XML 命名空間中的對等標籤
- `SPEKE:ProtectionHeader` 已棄用，並以 取代 `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`、 `SPEKE:KeyFormat`和 `SPEKE:KeyFormatVersions` 已棄用，並由 取代 `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id` 已由 取代 `CPIX@contentId`
- 新的強制性 CPIX 屬性：`CPIX@version`、 `ContentKey@commonEncryptionScheme`
- 新的選用 CPIX 元素： `DRMSystem.ContentProtectionData`
- 支援多個內容金鑰
- SPEKE 和 CPIX 之間的跨版本機制
- HTTP 標頭演變：新的`X-Speke-Version`標頭、重新命名為 的`Speke-User-Agent`標頭 `X-Speke-User-Agent`
- 心跳 API 棄用

隨著 SPEKE v1.0 規格保持不變，現有的實作不需要變更，即可繼續支援 SPEKE v1.0 工作流程。

主題

- SPEKE API v2 - DASH-IF 規格的自訂和限制
- SPEKE API v2 - 標準承載元件
- SPEKE API v2 - 加密合約

- SPEKE API v2 - 即時工作流程方法呼叫範例
- SPEKE API v2 - VOD 工作流程方法呼叫範例
- SPEKE API v2 - 內容金鑰加密
- SPEKE API v2 - 覆寫金鑰識別符

SPEKE API v2 - DASH-IF 規格的自訂和限制

DASH 產業論壇 CPIX 2.3 規格支援多種使用案例和拓撲。SPEKE API 2.0 版規格同時定義 CPIX 設定檔和 CPIX 的 API。為了實現這兩個目標，它遵循 CPIX 規格，具有下列自訂和限制條件：

CPIX 設定檔

- SPEKE 遵循 Encryptor Consumer 工作流程。
- 對於加密的內容金鑰，SPEKE 會套用下列限制：
  - SPEKE 不支援請求或回應承載的數位簽章驗證 (XMLDSIG)。
  - SPEKE 需要 2048 RSA 型憑證。
- SPEKE 只會利用一部分的 CPIX 功能：
  - SPEKE 會省略 `UpdateHistoryItemList`功能。如果回應中有清單，SPEKE 會忽略清單。
  - SPEKE 會省略根/分葉金鑰功能。如果`ContentKey@dependsOnKey`屬性存在於回應中，SPEKE 會忽略它。
  - SPEKE 會省略 `BitrateFilter`元素和 `VideoFilter@wcg` 屬性。如果這些元素或屬性存在於 CPIX 承載中，SPEKE 會忽略它。
- 只有在標準承載元件頁面或加密合約頁面中參考為「支援」的元素或屬性，才能用於與 SPEKE v2 交換的 CPIX 文件。
- 當加密程式包含在 CPIX 請求中時，所有元素和屬性都應在金鑰提供者 CPIX 回應中攜帶有效值。如果沒有，加密程式應停止並擲回錯誤。
- SPEKE 支援具有 `KeyPeriodFilter` 元素的金鑰輪換。SPEKE 僅使用 `ContentKeyPeriod@index`來追蹤金鑰期間。
- 對於 HLS 訊號，必須使用多個`DRMSystem.HLSSignalingData`元素：一個`DRMSystem.HLSSignalingData@playlist`屬性值為「媒體」，另一個`DRMSystem.HLSSignalingData@playlist`屬性值為「主要」。
- 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。
- 加密程式應包含 CPIX@contentId 屬性的值。接收此屬性的空值時，金鑰提供者應傳回描述為「遺失 CPIX@contentId」的錯誤。 CPIX@contentId值無法由金鑰提供者覆寫。

  CPIX@id 如果不是 null，則金鑰提供者應忽略 值。
- 加密程式應包含 CPIX@version 屬性的值。接收此屬性的空值時，金鑰提供者應傳回描述為「缺少 CPIX@version」的錯誤。收到具有不支援版本的請求時，金鑰提供者傳回的錯誤描述應為「不支援的 CPIX@version」。

  CPIX@version 值無法由金鑰提供者覆寫。
- 加密程式應包含每個請求金鑰ContentKey@commonEncryptionScheme屬性的值。接收此屬性的空值時，金鑰提供者應傳回描述為 'Missing ContentKey@commonEncryptionScheme for KID ' id 的錯誤。

  唯一的 CPIX 文件無法混合不同ContentKey@commonEncryptionScheme屬性的多個值。接收這類組合時，金鑰提供者應傳回描述為「不合規 ContentKey@commonEncryptionScheme 組合」的錯誤。

  並非所有ContentKey@commonEncryptionScheme值都與所有 DRM 技術相容。接收這類組合時，金鑰提供者應傳回描述為 'ContentKey@commonEncryptionScheme 且與 DRMSystem id ' 不相容的錯誤。

  ContentKey@commonEncryptionScheme 值無法由金鑰提供者覆寫。
- 在 CPIX 回應內文中接收 DRMSystem@PSSH和 DRMSystem.ContentProtectionData innerXML <pssh>元素的不同值時，加密程式應停止並擲回錯誤。 innerXML

CPIX 的 API

- 金鑰提供者應包含 X-Speke-User-Agent HTTP 回應標頭的值。
- 符合 SPEKE 的加密程式做為用戶端，並將 POST 操作傳送至金鑰提供者端點。
- 加密程式應包含 X-Speke-Version HTTP 請求標頭的值，搭配請求使用的 SPEKE 版本，配方為 MajorVersion.MinorVersion,例如 SPEKE v2.0 的 '2.0'。如果金鑰提供者不支援加密程式用於目前請求的 SPEKE 版本，金鑰提供者應傳回描述為「不支援的 SPEKE 版本」的錯誤，且不會盡力處理 CPIX 文件。

  加密程式定義的X-Speke-Version標頭值無法由金鑰提供者在回應請求時修改。

- 在回應內文中收到錯誤時，加密程式應該擲回錯誤，而不是使用 SPEKE v1.0 版本控制重試請求。

  如果金鑰提供者未傳回錯誤，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。

下表摘要說明必須由訊息內文中的金鑰提供者傳回的標準訊息。錯誤情況下的 HTTP 回應碼應為 4XX 或 5XX，而非 200。422 錯誤碼可用於與 SPEKE/CPIX 相關的所有錯誤。

錯誤案例	錯誤訊息
未定義 CPIX@contentId	缺少 CPIX@contentId
未定義 CPIX@version	缺少 CPIX@version
不支援 CPIX@version	不支援的 CPIX@version
未定義 ContentKey@commonEncryption Scheme	缺少 KID 的 ContentKey@commonEncryption Scheme `id`（其中 `id`等於 ContentKey@kid 值）
單一 CPIX 文件中使用的多個 ContentKey@commonEncryptionScheme 值	不合規的 ContentKey@commonEncryption Scheme 組合
ContentKey@commonEncryptionScheme 與 DRM 技術不相容	ContentKey@commonEncryptionScheme 與 DRMSystem 不相容 `id`（其中 `id`等於 DRMSystem@systemId 值）
X-Speke-Version 標頭值不是支援的 SPEKE 版本	不支援的 SPEKE 版本
加密合約格式錯誤	格式錯誤的加密合約
加密合約與 DRM 安全層級限制相抵觸	不支援請求的 CPIX 加密合約
加密合約不包含任何 VideoFilter 或 AudioFilter 元素	缺少 CPIX 加密合約

SPEKE API v2 - 標準承載元件

透過單一 SPEKE 請求，加密程式可以請求多個內容金鑰，以及多個封裝格式的必要 Manfest 訊號，根據指定內容定義的加密合約。

為了涵蓋所有這些層面，標準 CPIX 文件包含三個強制性清單區段，以及即時內容金鑰輪換的選用清單區段。

<cpix：ContentKeyList> 區段和頂層 <cpix：CPIX> 元素

這是必要區段，與即時串流和 VOD 串流相關，可定義加密程式需要使用的不同內容金鑰。<cpix:ContentKeyList> 元素可以包含一或多個<cpix:ContentKey>子元素，每個元素都會描述不同的內容金鑰。

根據 CPIX 規格，ContentKey@commonEncryptionScheme屬性的可能值會在 ISO 基礎媒體檔案格式檔案規格 (ISO/IEC 23001-7：2016) 的通用加密中定義：

- 'cenc'：AES-CTR 模式完整範例和影片 NAL 子範例加密
- 'cbc1'：AES-CBC 模式完整範例和影片 NAL 子範例加密
- 'cens'：AES-CTR 模式部分影片 NAL 模式加密
- 'cbcs'：AES-CBC 模式部分視訊 NAL 模式加密

下列範例顯示具有單一、未加密內容金鑰的 CPIX 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>
```

根據預設，內容金鑰不會加密，如以下範例所示。但是，加密程式可以透過包含 <cpix：DeliveryDataList> 元素來請求加密內容金鑰。如需詳細資訊，請參閱內容金鑰加密一節。

SPEKE 支援的元素	必要屬性	選擇性屬性	必要子元素	選用子元素
<cpix：CPIX>	contentId、版本、xmlns：cpix、xmlns：pskc	name， xmlns：enc	一個 <cpix：ContentKeyList>、一個 <cpix：DRMSystemList>、一個 <cpix：ContentKeyUsageRuleList>	一個 <cpix：DeliveryDataList>，一個 <cpix：ContentKeyPeriodList>
<cpix：ContentKeyList>	-	id	至少一個 <cpix：ContentKey>	-
<cpix：ContentKey>	kid、commonEncryptionScheme、Data	ID、演算法、explicitIV	一個 <pskc：Secret>	-
<pskc：Secret>	PlainValue 或 EncryptedValue	ValueMAC	-	<enc：EncryptionMethod>、<enc：CipherData>

<cpix：DRMSystemList> 區段

這是必要區段，與即時串流和 VOD 串流相關，定義需要與內容金鑰搭配使用的不同 DRM 系統。

下列範例顯示具有單一 PlayReady DRM 系統規格的 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>
```

如需 DRM systemIDs 的完整清單，請參閱 DASH-IF 識別符儲存庫的內容保護一節。

SPEKE 支援的元素	必要屬性	選擇性屬性	必要子元素	選用子元素
<cpix：DRMSystemList>	-	id	至少一個 <cpix：DRMSystem>	-
<cpix：DRMSystem>	kid、systemId	ID、名稱、PSSH	-	ContentProtectionData、SmoothStreamingProtectionHeaderData、兩個具有不同播放清單屬性值的 <cpix：HLSSignalingData> 元素

DRMSystem@PSSH 如果 ISO-BMFF 封裝已套用至媒體區段，則為強制性。加密程式只會將 DRMSystem.ContentProtectionData innerXML <pssh>元素用於資訊清單訊號。

如果 DRMSystem@PSSH 存在且DRMSystem.ContentProtectionData包含 innerXML <pssh>元素，則兩個值應相同。

如果要在 HLS 資訊清單中傳送DRMSystem訊號，則必須在 CPIX 請求<cpix:HLSSignalingData playlist="media">和回應中同時包含 和 <cpix:HLSSignalingData playlist="master">元素。

<cpix：ContentKeyPeriodList> 區段

這是選用區段，僅適用於即時串流，定義套用至內容的加密期間。

<cpix:ContentKeyPeriodList> 元素可以包含一或多個<cpix:ContentKeyPeriod>子元素，每個元素都會在即時時間軸中描述不同的加密期間。使用 UUIDs 做為 ID 屬性值的一部分，是常用的方法。

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

SPEKE 支援的元素	必要屬性	選擇性屬性	必要子元素	選用子元素
<cpix：ContentKeyPeriodList>	-	id	至少一個 <cpix：ContentKeyPeriod>	-
<cpix：ContentKeyPeriod>	ID、索引	-	-	-

如果使用加密期間，則加密金鑰也需要連接到 CPIX 文件的其中一個加密期間，如以下章節所示。

<cpix：ContentKeyUsageRuleList> 區段

這是必要區段，與即時串流和 VOD 串流相關，定義不同的內容金鑰如何在串流集中和加密期間保護軌跡。

<cpix：ContentKeyUsageRuleList> 元素可以包含一或多個 <cpix：ContentKeyUsageRule> 子元素，每個元素描述加密程式套用指定內容金鑰的軌道，可能在特定加密期間。至少需要一個 <cpix：AudioFilter> 或一個 <cpix：VideoFilter> 元素，才能存在於 <cpix：ContentKeyUsageRule> 元素中。

下列範例顯示一個簡單的清單，其中只有一個規則在特定加密期間將單一內容金鑰套用至所有音訊和視訊音軌。

```
<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>
```

SPEKE 支援的元素	必要屬性	選擇性屬性	必要子元素	選用子元素
<cpix：ContentKeyUsageRuleList>	-	id	至少一個 <cpix：ContentKeyUsageRule>	-
<cpix：ContentKeyUsageRule>	kid， intendedTrackType	-	至少一個 <cpix：AudioFilter> 或一個 <cpix：VideoFilter> (*)	<cpix：KeyPeriodFilter>
<cpix：KeyPeriodFilter>	periodId	-	-	-
<cpix：AudioFilter>	-	minChannels、maxChannels	-	-
<cpix：VideoFilter>	-	minPixels、maxPixels、hdr、minFps、maxFps	-	-

(*) 如需使用單一或多個內容金鑰來保護串流集中一或多個音軌的詳細說明，請參閱加密合約文件一節。_

SPEKE API v2 - 加密合約

加密合約會根據軌跡特性，定義哪些內容金鑰正在保護指定串流集中的追蹤。

使用多個內容索引鍵處理串流集中的不同音軌，雖然這是建議的產業最佳實務，但不是強制性的，但建議使用 - 至少兩個不同的內容索引鍵，一個用於音訊音軌，另一個用於視訊音軌。可以使用單一內容金鑰來加密多個軌道，但需要在加密程式傳送至金鑰提供者的 CPIX 文件中明確發出訊號。一般而言，加密器一律會準確描述需要多少內容金鑰，以及如何利用這些金鑰來加密各種媒體軌跡。

原則

加密合約位於 CPIX 文件的 <cpix:ContentKeyUsageRuleList>區段。
在本節中， <cpix:ContentKeyList> 區段中定義的每個內容金鑰對應至特
定<cpix:ContentKeyUsageRule>元素，其中應包含：

- 可以參考一或多個子元件的ContentKeyUsageRule@intendedTrackType屬性，如果使用多個子元件，則以「+」符號分隔。的值ContentKeyUsageRule@intendedTrackType在加密合約中應是唯一的，不能用於多個ContentKeyUsageRule元素。
- 一或多個<cpix:AudioFilter>或<cpix:VideoFilter>子元素，取決於ContentKeyUsageRule@intendedTrackType屬性的值。

管理此關係的規則如下：

- 當串流集的所有音訊和視訊音軌都需要使用唯一的內容金鑰保護時，'ALL'必須使用字串做為ContentKeyUsageRule@intendedTrackType屬性值。範例 1 顯示這類使用案例。在這種情況下，應同時包含不含任何屬性的 <cpix:AudioFilter />和<cpix:VideoFilter />子元素。<cpix:AudioFilter> 和/或<cpix:VideoFilter>元素的任何其他組合在此特定內容中無效。
- 對於所有其他使用案例，可以自由定義ContentKeyUsageRule@intendedTrackType屬性的值，且 <cpix:AudioFilter />和<cpix:VideoFilter />子元素的數量必須對應至透過 '+' 符號彙總的子元件數量。當ContentKeyUsageRule@intendedTrackType屬性值中存在單一子元件時，範例 2/3/4/5/6/7/9/10 會說明此要求。範例 8 說明使用多個子元件時的情況：由具有不同屬性值的兩個不同<cpix:VideoFilter>子元素ContentKeyUsageRule@intendedTrackType="SD+HD"描述，以及由具有不同屬性值的三個不同<cpix:VideoFilter>子元素ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"描述。

篩選條件

CPIX 定義多個篩選元素和屬性，但 SPEKE 僅支援其中一部分。下表摘要說明這些差異：

CPIX 篩選條件類型	整體 SPEKE 支援	SPEKE 支援的篩選條件屬性	SPEKE 不支援篩選條件屬性
<cpix：VideoFilter>	是	minPixels、maxPixels、hdr、min	wcg

CPIX 篩選條件類型	整體 SPEKE 支援	SPEKE 支援的篩選條件屬性	SPEKE 不支援篩選條件屬性
		Fps、maxFps（選用屬性）	
<cpix：AudioFilter>	是	minChannels、maxChannels（選用屬性）	
<cpix：KeyPeriodFilter>	是	periodId（必要屬性）	
<cpix：BitrateFilter>	否	N/A	N/A
<cpix：LabelFilter>	否	N/A	N/A

根據 VideoFilter 的 CPIX 規格，【minPixels， maxPixels】 是兩個維度中所有包含的範圍，而 (minFps， maxFps】 僅包含 maxFps 維度。對於 AudioFilter，【minChannels， maxChannels】 是兩個維度中的包含範圍。

有問題的情況

在某些情況下，加密合約中提供的資訊可能是部分、不明確或錯誤。在這些情況下，加密程式和金鑰提供者必須正確運作，並保證對內容提供適當的保護。下表顯示在這些情況下的建議行為：

在這種情況下	加密程式應該/應...	金鑰提供者應...
沒有規則適用於串流集中的一或多個音軌（請參閱下列範例 3)	加密程式應查看其組態 (CPIX 承載外部），並確認相關軌道不需要加密。如果不是預期，加密程式應該擲回錯誤並停止處理。	不相關：金鑰提供者不了解串流集結構。
多個規則重疊，並建議多個內容金鑰來加密特定軌道	加密程式應依照文件的順序，套用最後一個已成功評估的 ContentKeyUsageRule。	不相關：金鑰提供者不了解串流集結構。

在這種情況下	加密程式應該/應...	金鑰提供者應...
加密合約會在單一 SPEKE 請求/回應週期中變更	加密程式應提出例外狀況並停止處理，因為金鑰提供者不負責定義加密合約。	為了防止這種情況一開始發生，金鑰提供者不得修改 SPEKE 請求的 CPIX 承載中收到的加密合約。
格式錯誤的加密合約：intendedTrackType/Filters 基數限制條件例外狀況、不支援的篩選條件或屬性	加密程式應提出例外狀況、停止處理，且不會將 SPEKE 請求傳送給金鑰提供者，因為這很可能會導致內容保護錯誤或讓某些軌跡處於未受保護的狀態。	金鑰提供者應提出例外狀況並傳回「格式化加密合約」錯誤。
形式良好的加密合約，但違反 DRM 安全層級限制：例如，為保護音訊音軌和 UHD 視訊音軌而請求的單一內容金鑰	如果加密程式了解 DRM 安全層級限制，應引發例外狀況、停止處理，而且不會將 SPEKE 請求傳送給金鑰提供者，因為這很可能會導致內容保護錯誤。	金鑰提供者應提出例外狀況，並傳回不支援的「請求 CPIX 加密合約」錯誤。
缺少加密合約	加密程式不應傳送不包含任何 VideoFilter 或 AudioFilter 元素的 CPIX 文件。	金鑰提供者應提出例外狀況，並傳回「缺少 CPIX 加密合約」錯誤。

加密合約的範例

範例 1：一個內容金鑰，用於所有音訊和視訊音軌

```
<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 2：一個內容金鑰用於所有影片音軌，一個內容金鑰用於所有音訊音軌

```
<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: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 3：一個內容索引鍵，用於所有影片音軌、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：多個內容金鑰用於不同的影片音軌 (SD/HD)，一個內容金鑰用於所有音訊音軌

```
<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：多個內容金鑰用於不同的影片音軌 (SD/HD/UHD)，一個內容金鑰用於所有音訊音軌

```
<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：適用於不同影片音軌的多個內容金鑰 (SD/HD/UHD1/UHD2)，一個內容金鑰適用於所有音訊音軌

```
<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：適用於不同影片音軌的多個內容金鑰 (SD/HD1/HD2/UHD1/UHD2)，一個內容金鑰用於所有音訊音軌

```
<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：適用於不同視訊音軌的多個內容金鑰（根據多個屬性類型）、適用於所有音訊音軌的單一內容金鑰

```
<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 9：一個內容金鑰用於所有影片音軌，多個內容金鑰用於立體聲和多聲道音訊音軌

```
<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-->
 <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 10：一個內容金鑰用於所有影片音軌、多個內容金鑰用於立體聲，以及兩種多頻道音軌類型

```
<cpix:ContentKeyUsageRuleList>
 <!-- Rule for video tracks-->
 <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
```

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

SPEKE API v2 - 即時工作流程方法呼叫範例

請求語法範例

下列 URL 範例僅供參考，格式並非固定不變：

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

請求內文

CPIX 文件。

請求標頭

名稱	Type	發生	描述
`AWS Authorization`	字串	1..1	請參閱 AWS Sigv4

名稱	Type	發生	描述
X-Amz-Security-Token	字串	1..1	請參閱 AWS Sigv4
X-Amz-Date	字串	1..1	請參閱 AWS Sigv4
Content-Type	字串	1..1	application/xml
X-Speke-Version	字串	1..1	與請求搭配使用的 SPEKE API 版本，配方為 MajorVersion.MinorVersion,例如 SPEKE 2.0 版的 '2.0'

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	與請求搭配使用的 SPEKE API 版本，配方為 MajorVersion.MinorVersion,例如 SPEKE 2.0 版的 '2.0'

請求回應

HTTP 代碼	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 承載回應

HTTP 代碼	承載名稱	發生	描述
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器到 DRM 金鑰提供者的典型即時請求承載，所有視訊追蹤有一個內容金鑰，所有音訊追蹤一個內容金鑰：

```
<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承載（傳回的值已縮短為 【... 】 以保證可讀性）：

```
<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>
```

SPEKE API v2 - VOD 工作流程方法呼叫範例

請求語法範例

下列 URL 範例僅供參考，格式並非固定不變。

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

請求內文

CPIX 文件。

請求標頭

名稱	Type	發生	描述
AWS Authorization	字串	1..1	請參閱 AWS Sigv4
X-Amz-Security-Token	字串	1..1	請參閱 AWS Sigv4
X-Amz-Date	字串	1..1	請參閱 AWS Sigv4
Content-Type	字串	1..1	application/xml
X-Speke-Version	字串	1..1	與請求搭配使用的 SPEKE API 版本，配方為 MajorVersion.MinorVersion,例如 SPEKE 2.0 版的 '2.0'

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	與請求搭配使用的 SPEKE API 版本，配方為 MajorVersion.MinorVersion,例如 SPEKE 2.0 版的 '2.0'

請求回應

HTTP 代碼	承載名稱	發生	描述
200 (Success)	CPIX	1..1	DASH-CPIX 承載回應
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資訊，請參閱內容金鑰加密。

清除中包含金鑰的 VOD 範例請求承載

下列範例顯示從加密器到 DRM 金鑰提供者的典型 VOD 請求承載，所有視訊追蹤有一個內容金鑰，所有音訊追蹤一個內容金鑰：

```
<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>
```

清除中包含金鑰的 VOD 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承載（傳回的值已縮短為 【... 】 以保證可讀性）：

```
<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>
```

SPEKE API v2 - 內容金鑰加密

您可以選擇性地將內容金鑰加密新增至 SPEKE 實作。除了加密內容本身外，內容金鑰加密還會透過加密內容金鑰進行傳輸，以確保完整的端對端保護。如果您未為金鑰提供者實作此項目，則需依賴傳輸層加密加上強式身分驗證以確保安全。

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

限制

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

- SPEKE 不支援請求或回應承載的數位簽章驗證 (XMLDSIG)。
- SPEKE 需要 2048 RSA 型憑證。

這些限制也會列在自訂和 DASH-IF 規格的限制中。

實作內容金鑰加密

若要提供內容金鑰加密，請在您的 DRM 金鑰提供者實作中包含下列內容：

- 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>
```

SPEKE API v2 - 覆寫金鑰識別符

加密程式會在每次輪換金鑰時建立新的金鑰識別符 (KID)。它會在請求中將 KID 傳遞到 DRM 金鑰提供者。金鑰提供者通常會使用相同的 KID 進行回應，但它可以為回應中的 KID 提供不同的值。

下列是 KID 的範例請求 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>
```

下列回應會將 KID 覆寫為 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>
```

SPEKE API 規格的授權

Creative Commons Attribution-ShareAlike 4.0 國際公有授權

透過行使授權權利（定義如下），您接受並同意受此 Creative Commons Attribution-ShareAlike 4.0 國際公有授權 (「公有授權」) 的條款與條件約束。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. 轉接器的授權表示您根據此公有授權的條款與條件，在對改編資料做出貢獻時，適用於您的著作權和類似權利的授權。

c. BY-SA 相容授權是指列於 https：//creativecommons.org/compatiblelicenses。

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. 有效科技措施係指雖無未經適當授權，但依據法律不得規避 1996 年 12 月 20 日 WIPO 著作權條約第 11 條及/或其他相似國際協定規範義務履行之措施。

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. License Elements 表示列於 Creative Commons 公有授權名稱中的授權屬性。此公有授權的授權元素是屬性和 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. 全部或部分重製和共用授權素材；以及

   B. 產生、重製和共用調整後的資料。

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. 授權方提供的其他優惠 – 調整後的資料。您改編資料的每個收件人都會自動收到授權方的優惠，以在您所套用轉接器授權的條件下，在改編資料中行使授權權利。

   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. 如果授權方隨授權素材提供，則保留下列項目：

```
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. 指出您是否已修改授權素材，並保留任何先前修改的指示；以及

C. 表示授權素材已依此公有授權授權，並包含此公有授權的文字、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，藉由提供 URI 或提供包含必要資訊之資料來源的超連結，可認定為合理滿足此條件。
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) 節中的條件之外，如果您共享您生產的改編材料，也適用下列條件。

1. 您套用的轉接器授權必須是具有相同授權元素、此版本或更新版本的 Creative Commons 授權，或是 BY-SA 相容授權。
2. 您必須包含您所套用轉接器授權的文字、URI 或超連結。您可以根據您共用調整後材料的媒介、方式和內容，以任何合理的方式滿足此條件。
3. 您不得提供或強加任何額外或不同的條款或條件，或套用任何有效的技術措施至修改後的資料，以限制依據您套用的轉接器授權所授予之權利的行使。

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) 節授予您擷取、重複使用、重製和共用資料庫全部或部分內容的權利；

b. 如果您在擁有 Sui Generis 資料庫權利的資料庫中包含所有或大部分的資料庫內容，則您擁有 Sui Generis 資料庫權利（但非其個別內容）的資料庫為調整後材料，包括第 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. 自違規改正日期起自動改正，但前提是該違規在您發現後 30 天內改正；或

   2. 授權方明確恢復時。

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中 SPEKE 支援的新章節，列出 Bitmovin 服務。	2023 年 1 月 13 日
DRM 平台供應商的更新	將連結和新的合作夥伴資訊新增至 DRM 平台供應商清單。	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，安全封裝程式和編碼器金鑰交換僅支援透明金鑰交付。	2018 年 10 月 30 日
支援矩陣 - AWS Elemental Live	新增 AWS Elemental Live 支援矩陣。	2018 年 9 月 27 日
標準承載元件	新增定義 JSON 承載中主要元素的章節。	2018 年 9 月 27 日
KID 覆寫	新增金鑰提供者覆寫 KID 的章節。	2018 年 9 月 27 日
更正 DASH-IF 網站的連結	更正 CPIX 規定和系統 ID 頁面的 DASH IF 網站連結。	2018 年 9 月 27 日
AWS Elemental Live 的版本副本	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	更新服務的支援矩陣表格，以包括常見的媒體應用程式格式 (CMAF)。	2018 年 6 月 27 日
初始版本	安全封裝程式和編碼器金鑰交換 (SPEKE) 第 1 版的初始版本，這是內容加密程式與 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
更新 DRM 平台提供者區段，以及支援 SPEKE 的 AWS 服務和產品區段	將 Webstream 新增至 DRM 平台提供者清單的 SPEKE v2 欄，將 MediaConvert 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	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的 X-Speke-Version 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	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	2022 年 1 月 27 日

變更	描述	日期
	密合約的新範例，並在所有相關範例中將 SD 最大解析度變更為 1024x576。	
初始版本	安全封裝程式和編碼器金鑰交換 (SPEKE) 2.0 版的初始版本，內容加密程式與 DRM 金鑰提供者之間的通訊規格。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。