合作伙伴和客户指南

安全包装程序和编码器密钥交换 API 规范

Copyright © 2021 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

安全包装程序和编码器密钥交换 API 规范: 合作伙伴和客户指南

Copyright © 2021 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

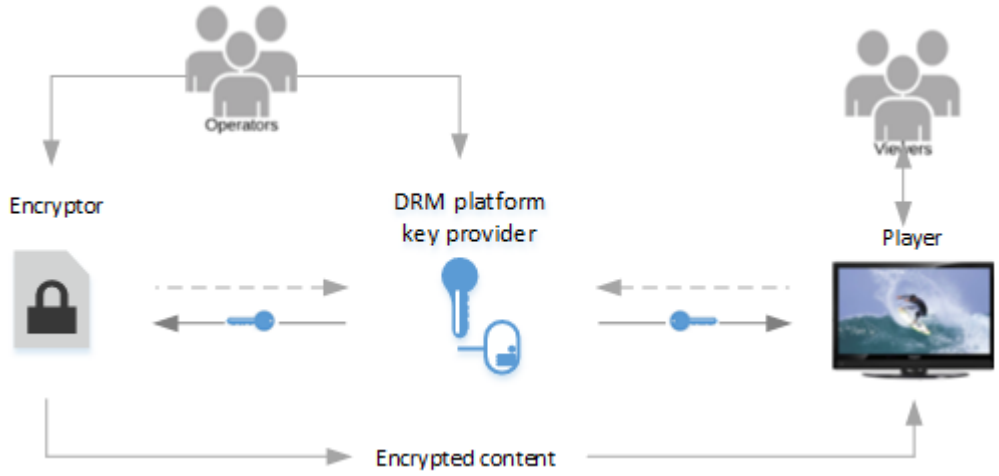
什么是安全包装程序和编码器密钥交换？

安全包装程序和编码器密钥交换 (SPEKE) 定义加密程序与媒体内容的包装程序以及数字版权管理 (DRM) 密钥提供程序之间的通信标准。该规范适用于在本地和 AWS 云中运行的加密器。

主题

常规架构

下图显示了内部产品的 SPEKE 内容加密架构的高级视图。

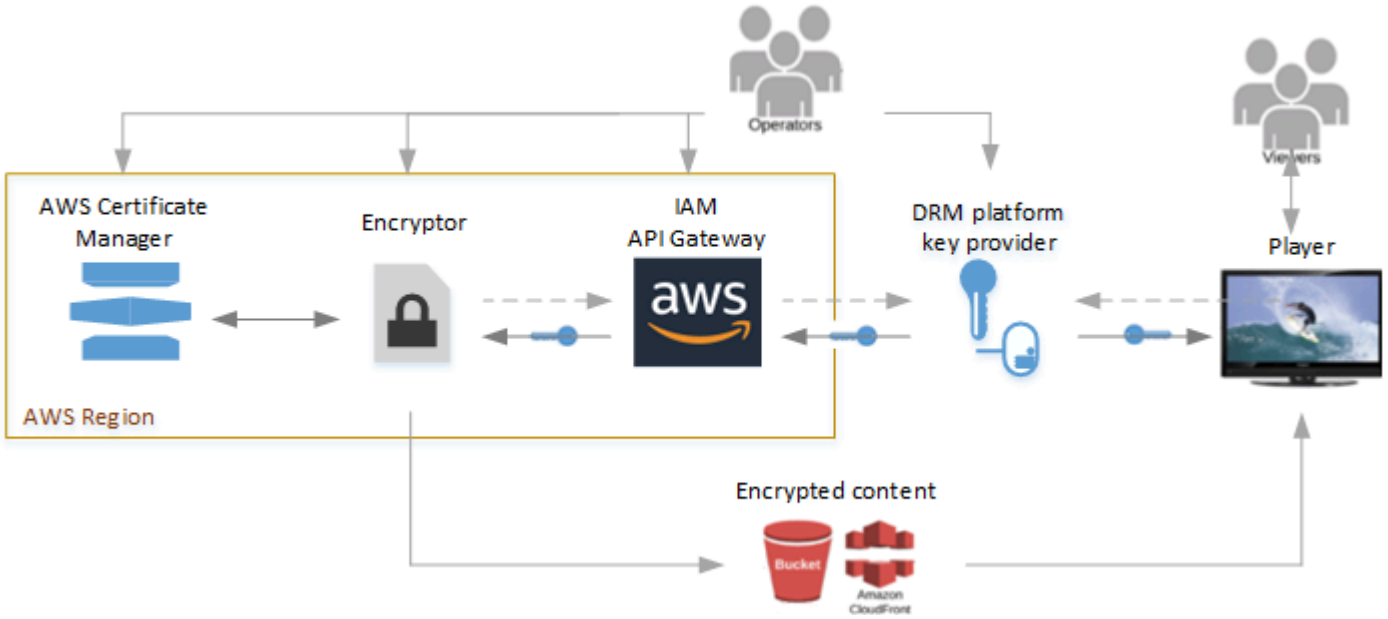


以下是上述架构的主要组件：

- 加密程序 – 提供加密技术。接收来自其操作人员的加密请求，并从 DRM 密钥提供程序检索所需密钥以保护加密内容。
- DRM 平台密钥提供程序 – 通过符合 SPEKE 规范的 API 将加密密钥提供给加密程序。此外，提供程序将许可证提供给媒体播放器以进行解密。
- 播放器 – 请求来自同一 DRM 平台密钥提供程序的密钥，播放器将使用该密钥解锁内容并将内容提供给查看者。

基于 AWS 云的架构

下图显示将 SPEKE 与在 AWS 云中运行的服务和功能 结合使用时的高级架构。



以下是主要服务和组件：

- 加密程序 – 在 AWS 云中提供加密技术。加密程序接收来自其操作人员的请求，并通过 Amazon API Gateway 从 DRM 密钥提供程序检索所需加密密钥以保护加密的内容。它会将加密的内容传输到 Amazon S3 存储桶或通过亚马逊 CloudFront 分发。
- AWS IAM 和 Amazon API Gateway – 管理客户信任的角色以及加密程序与密钥提供程序之间的代理通信。API Gateway 提供日志记录功能，使客户能够控制其与加密程序以及 DRM 平台之间的关系。客户通过 IAM 角色配置实现密钥提供程序访问。API Gateway 必须与加密器位于相同的 AWS 区域。
- AWS Certificate Manager – (可选) 提供针对内容密钥加密的证书管理。要确保通信安全，建议的做法是加密内容密钥。证书管理器必须位于加密程序所在的同一 AWS 区域中。
- DRM 平台密钥提供程序 – 通过符合 SPEKE 规范的 API 将加密密钥提供给加密程序。此外，提供程序将许可证提供给媒体播放器以进行解密。
- 播放器 – 请求来自同一 DRM 平台密钥提供程序的密钥，播放器将使用该密钥解锁内容并将内容提供给查看者。

如何开始

有关 SPEKE 的更多介绍材料，请参阅 SPEKE 的新用户？。

您是客户吗？

与 AWS Elemental DRM 平台提供商合作以开始使用加密。有关详细信息，请参阅客户登记。

您是 DRM 平台提供商还是具有自己的密钥提供程序的客户？

根据 SPEKE 规范，公开密钥提供程序的 REST API。有关详细信息，请参阅 SPEKE API 规范。

SPEKE 的新用户？

本节为刚开始使用 Secure Packager 和 Encoder Key Exchange (SPEKE) 的读者提供入门信息。

有关 SPEKE 的介绍，请观看以下网络广播：

相关服务信息和规格

- API 网关权限 – 如何使用 AWS Identity and Access Management（AWS IAM）控制对 API 的访问。
- AWS AssumeRole — 如何使用 AWS Security Token Service (AWS STS) 来承担角色功能。
- AWS Sigv4 – 如何使用签名版本 4 为 HTTP 请求签名。
- DASH-IF CPIX 规范 v2.0 – DASH-IF 内容保护信息交换格式（CPIX）规范（此 SPEKE v1.0 规范的基础）。
- DASH-IF CPIX 规范 v2.3 – DASH-IF 内容保护信息交换格式（CPIX）规范（此 SPEKE v2.0 规范的基础）。
- DASH-IF 系统 IDs — DRM 系统的注册标识符列表。
- https://github.com/awslabs/speke-reference-server— 示例参考密钥提供商，用于您的 AWS 账户，以帮助您开始在 AWS 中实施 SPEKE。

术语

以下列表定义了本规范中使用的术语。在可能的情况下，本规范遵循 DASH-IF CPIX 规范中使用的术语。

- ARN – Amazon 资源名称。唯一地标识 AWS 资源。
- 内容密钥 – 用于加密一部分内容的加密密钥。
- 内容提供商 – 提供针对受保护媒体的传输的权限和规则的发布者。内容提供者还可能提供源媒体（夹层格式，用于转码）、资产标识符、密钥标识符 (KIDs)、密钥值、编码指令和内容描述元数据。
- DRM – 数字权限管理。用于保护受版权保护的数字内容免受未经批准的访问。
- DRM 平台 – 为内容加密程序和查看器提供 DRM 功能和支持的系统，包括提供用于对内容进行加密和解密的 DRM 密钥和许可。

- DRM 提供商 – 请参阅 DRM 平台。
- DRM 系统 – DRM 实施标准。常见的 DRM 系统包括苹果 FairPlay、谷歌 Widevine 和微软。PlayReady内容提供商使用 DRM 系统来保护数字内容以便传送给查看者和供查看者访问。有关在 DASH-IF 中注册的 DRM 系统的列表，请参阅 DASH-IF 系统。 IDsDASH-IF CPIX 规范使用此处定义的术语“DRM 系统”，在某些地方，它使用“DRM 系统”来表示此规范将哪些内容称为 DRM 平台。
- DRM 解决方案 – 请参阅 DRM 平台。
- DRM 技术 – 请参阅 DRM 系统。
- 加密程序 – 一种媒体处理组件，它使用从密钥提供程序处获得的密钥加密媒体内容。加密程序通常还会向媒体添加 DRM 加密信令和元数据。加密程序通常是编码器、包装程序和转码器。
- 密钥提供程序 – DRM 平台的一个组件，它公开 SPEKE REST API 以处理密钥请求。密钥提供程序可能是密钥服务器本身，也可能是平台的另一个组件。
- 密钥服务器 – DRM 平台的一个组件，用于维护内容加密和解密的密钥。
- 操作人员 – 负责操作整个系统（包括加密程序和密钥提供程序）的人员。
- 播放器 – 代表查看者运行的媒体播放器。获取来自其他源（包括媒体清单文件、媒体文件和 DRM 许可证）的信息。代表查看者从 DRM 平台请求许可证。

SPEKE 的客户入职培训

通过将安全包装程序和编码器密钥交换（SPEKE）数字版权管理（DRM）系统提供商与您的加密程序以及媒体播放器组合在一起来保护您的内容，使其不会受到未经授权的使用。SPEKE 定义加密程序与媒体内容的包装程序以及数字版权管理（DRM）密钥提供程序之间的通信标准。要登记，您需要选择 DRM 平台密钥提供商并配置密钥提供商与加密程序和播放器之间的通信。

主题

开始使用 DRM 平台提供商

以下 Amazon 合作伙伴为 SPEKE 提供第三方 DRM 平台实施。有关其产品/服务的详细信息以及有关其联系方式的信息，请访问指向其 Amazon Partner Network 页面的链接。虽然不具有链接的合作伙伴当前没有 Amazon Partner Network 页面，但您可以直接联系他们。合作伙伴可以帮助您进行设置以使用他们的平台。

DRM 平台提供商	SPEKE v1 支持	SPEKE v2 支持
Axinom	√	√
BuyDRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
DOVERUNNER	√	√
Insys Cloud DRM	√	√
Intertrust Technologies	√	√

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

在 AWS 服务和产品中提供 SPEKE 支持

本节列出了在 AWS Cloud 中运行的 AWS 媒体服务和 AWS 本地媒体产品提供的 SPEKE 支持。这些服务和产品是 SPEKE 内容加密架构中的加密程序。确认您的流式处理协议和您希望对服务或产品可用的 DRM 系统。

AWS 服务或产品	SPEKE v1 支持	SPEKE v2 支持	支持的 DRM 技术
AWS Elemental MediaConvert — 在 AWS 云中运行的服务	√	√	文档
AWS Elemental MediaPackage — 在 AWS 云中运行的服务	√	√	文档
AWS Elemental Live- 本地产品	√		文档：MPEG-DASH / HLS

AWS 服务或产品	SPEKE v1 支持	SPEKE v2 支持	支持的 DRM 技术
AWS Elemental Server-本地产品	√		文档

在 AWS 合作伙伴服务和产品中提供 SPEKE 支持

本部分列出了在 AWS Cloud 中运行的 AWS 合作伙伴服务和产品提供的 SPEKE 支持。这些服务和产品是 SPEKE 内容加密架构中的加密程序。确认您的流式处理协议和您希望对服务或产品可用的 DRM 系统。

AWS 服务或产品	SPEKE v1 支持	SPEKE v2 支持	支持的 DRM 技术
Bitmovin 实时视频编码	√		文档
Bitmovin 点播视频（VOD）编码	√		文档

SPEKE API 规范

这是用于安全包装程序和编码器密钥交换（SPEKE）的 REST API 规范。使用此规范为使用加密的客户提供 DRM 版权保护。

在视频流式处理工作流中，加密引擎与 DRM 平台密钥提供程序通信以请求内容密钥。这些密钥是高度敏感的，因此，密钥提供程序和加密引擎建立高度安全的可信通信渠道是至关重要的。您还可以对文档中的内容密钥进行加 end-to-end密，以实现更安全的加密。

此规范可实现以下目标：

- 定义一个简单、可信、高度安全的接口，DRM 供应商和客户可以在需要内容加密时使用该接口与加密程序集成。
- 涵盖 VOD 和实时工作流，并包含对于加密程序和 DRM 密钥提供程序终端节点之间的可靠且高度安全的通信所需的错误条件和身份验证机制。
- 包括对 HLS、MSS 和 DASH 打包及其常用 DRM 系统的支持： FairPlay PlayReady、和 WideVine/CENC。
- 确保规范简单且可扩展以支持未来 DRM 系统。
- 使用简单的 REST API。

> **Note**
>
> 2021，Amazon Web Services, Inc. 或其附属公司版权所有。保留所有权利。
> 该文档根据知识共享署名-ShareAlike 4.0国际许可协议提供。
> 本规范中包含的材料按“原样”提供，无任何明示或暗示的保证，包括但不限于有关适销性、针对特定目的的适用性和不侵权的保证。任何情况下，此材料的作者或版权所有者都不应承担任何索赔、损害赔偿或其他责任，无论是因此材料或使用或其他材料处理引起的或与其相关的合同行为、侵权行为或其他行为。

主题

SPEKE 需要进行身份验证

SPEKE 要求对本地产品以及在 AWS 运行中运行的服务和功能进行身份验证。

主题

AWS 云实施的身份验证

SPEKE 要求通过 IAM 角色进行 AWS 身份验证以便与加密程序结合使用。IAM 角色由 DRM 提供商或拥有 AWS 账户中的 DRM 端点的操作人员创建。每个角色分配有一个 Amazon 资源名称（ARN），AWS Elemental 服务操作人员在请求加密时会在服务控制台上提供该名称。该角色的策略权限必须配置为授予访问密钥提供程序 API 的权限而不授予其他 AWS 资源访问权限。当加密程序联系 DRM 密钥提供程序时，它使用角色 ARN 代入密钥提供程序账户持有人的角色，从而返回临时凭证以供加密程序用于访问密钥提供程序。

一种常见的实施是操作人员或 DRM 平台供应商在密钥提供程序前使用 Amazon API Gateway，然后对 API Gateway 资源启用 AWS Identity and Access Management（AWS IAM）授权。您可以使用以下策略定义示例并将其附加到新角色以向相应资源授予权限。在此示例中，这些权限适用于所有 API Gateway 资源：

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

最后，该角色需要添加信任关系，并且操作人员必须能够选择服务。

以下示例显示为访问 DRM 密钥提供程序而创建的角色 ARN：

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

有关创建角色的更多信息，请参阅 AWS AssumeRole。有关对请求进行签名的更多信息，请参阅 AWS Sigv4。

本地产品的身份验证

对于本地产品，我们建议您使用 SSL/TLS 和摘要身份验证以获得最佳安全性，但至少应使用基于 HTTPS 的基本身份验证。

这两种身份验证都使用 HTTP 请求中的 `Authorization` 标头：

- 摘要式身份验证 – 授权标头包含标识符 `Digest`，其后一系列用于对请求进行身份验证的值。具体而言，响应值是通过一系列 MD5 哈希函数生成的，这些哈希函数包括来自 one-time-use服务器的唯一随机数，用于确保密码安全传输。
- 基本身份验证 – 授权标头包含标识符 `Basic`，其后是表示用户名和密码的 Base-64 编码的字符串（用冒号分隔）。

有关基本身份验证和摘要式身份验证的信息（包括有关标头的详细信息），请参阅 Internet Engineering Task Force (IETF) 规范 RFC 2617 - HTTP 身份验证：基本身份验证和摘要式访问身份验证。

SPEKE API v1

这是用于安全打包器和编码器密钥交换 (SPEKE) v1 的 REST API。使用此规范为使用加密的客户提供 DRM 版权保护。为了符合 SPEKE，您的 DRM 密钥提供程序必须公开本规范中描述的 REST API。加密程序对您的密钥提供程序进行 API 调用。

> **Note**
>
> 本规范中的代码示例仅用于说明目的。您无法运行这些示例，因为它们不是完整的 SPEKE 实现的一部分。

SPEKE 使用 DASH 行业论坛内容保护信息交换格式 (DASH-IF-CPIX) 数据结构定义进行密钥交换，但有一些限制。 DASH-IF-CPIX定义了一个架构，以提供从 DRM 平台到加密器的可扩展的多 DRM 交换。这使得在内容压缩和打包时允许对所有自适应比特率打包格式进行内容加密。自适应比特率打包格式包括 HLS、DASH 和 MSS。

有关交易格式的详细信息，请参阅达世币行业论坛CPIX规范，网址为 https://dashif。 org/docs/DASH-IF-CPIX-v2-0.pdf。

主题

SPEKE API v1 - 有关 DASH-IF 规范的自定义项和约束

DASH-IF CPIX 规范，https://dashif。 org/docs/DASH-IF-CPIX-v2-0.pdf，支持多种用例和拓扑。SPEKE API 规范符合具有以下自定义项和约束的 CPIX 规范：

- SPEKE 遵循 Encryptor Consumer 工作流。
- 对于加密的内容密钥，SPEKE 应用以下限制：
  - SPEKE 不支持请求或响应负载的数字签名验证（XMLDSIG）。
  - SPEKE 需要基于 2048 位 RSA 的证书。
- 对于轮换密钥工作流，SPEKE 需要 `ContentKeyUsageRule` 筛选条件 `KeyPeriodFilter`。SPEKE 会忽略所有其他 `ContentKeyUsageRule` 设置。
- SPEKE 会忽略 `UpdateHistoryItemList` 功能。如果响应中包含该列表，则 SPEKE 会将其忽略。
- SPEKE 支持密钥轮换。SPEKE 只使用 `ContentKeyPeriod@index 来跟踪关键时段。
- 为了支持 MSS PlayReady，SPEKE 在`DRMSystem`标签下使用了一个自定义参数。`SPEKE:ProtectionHeader`
- 对于 HLS 打包，如果 `URIExtXKey` 包含在响应中，则它必须包含要在 HLS 播放列表的 `EXT-X-KEY` 标签的 URI 参数中添加的完整数据，没有其他信号发送要求。
- 对于 HLS 播放列表，在 `DRMSystem` 标签下，SPEKE 提供了可选的自定义参数 `speke:KeyFormat` 和 `speke:KeyFormatVersions`，对应于 `EXT-X-KEY` 标签的 `KEYFORMAT` 和 `KEYFORMATVERSIONS` 参数的值。

HLS 初始化向量 (IV) 始终跟随段编号，除非由运算符显式指定。

- 当请求密钥时，加密程序可能会在 ContentKey 元素上使用可选的 @explicitIV 属性。密钥提供程序可以使用 @explicitIV 来响应 IV，即使该属性未包含在请求中。
- 加密程序创建密钥标识符 (KID)，这对于任何给定的内容 ID 和密钥周期保持不变。密钥提供程序在其对请求文档的响应中包含 KID。
- 密钥提供程序可能包含 Speke-User-Agent 响应标头的值以确定本身用于调试目的。
- 对于每个内容，SPEKE 目前不支持多个轨迹或密钥。

符合 SPEKE 的加密程序充当客户端并向密钥提供程序端点发送 POST 操作。加密程序可能会发送定期 heartbeat 请求，以确保加密程序和密钥提供程序终端节点之间的连接正常。

SPEKE API v1 - 标准负载组件

在任何 SPEKE 请求中，加密程序都可以请求针对一个或多个 DRM 系统的响应。加密程序在请求负载 <cpix:DRMSystemList> 中指定 DRM 系统。每个系统规范都包含密钥，并指示要返回的响应类型。

以下示例显示了一个 DRM 系统列表与单个 DRM 系统规范：

```
<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>
```

下表列出了每个 <cpix:DRMSystem> 的主要组件。

标识符	描述
systemId 或 schemeId	DRM 系统类型的唯一标识符，如在 DASH IF 组织中注册的。有关列表，请参阅 DASH-IF 系统。 IDs
kid	密钥 ID。这不是实际密钥，而是指向哈希表中的密钥的标识符。

标识符	描述
<cpix:UriExtXKey>	请求标准未加密密钥。密钥响应类型必须是此响应或 PSSH 响应。
<cpix:PSSH>	请求保护系统特定标头 (PSSH)。这种标头包含对 kid 的引用、systemID 以及 DRM 供应商的自定义数据（作为常见加密 (CENC) 的一部分）。密钥响应类型必须是此响应或 UriExtXKey 响应。

标准密钥和 PSSH 的示例请求

以下示例显示从加密程序到 DRM 密钥提供程序的示例请求的一部分，其中突出显示了主要组件。第一个请求针对的是标准密钥，第二个请求针对的是 PSSH 响应：

```
<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>
```

标准密钥和 PSSH 的示例响应

以下示例显示从 DRM 密钥提供程序到加密程序的相应响应：

SPEKE API v1 - 实时工作流方法调用示例

请求语法示例

以下 URL 是一个示例，并且不指示固定格式：

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

请求正文

CPIX 元素。

请求标头

名称	类型	发生次数	描述
`AWS Authorization`	字符串	1..1	请参阅 AWS Sigv4

名称	类型	发生次数	描述
X-Amz-Security-Token	字符串	1..1	请参阅 AWS Sigv4
X-Amz-Date	字符串	1..1	请参阅 AWS Sigv4
Content-Type	字符串	1..1	application/xml

响应标头

名称	类型	发生次数	描述
Speke-User-Agent	字符串	1..1	用于标识密钥提供程序的字符串
Content-Type	字符串	1..1	application/xml

请求响应

HTTP 代码	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 负载响应
4XX (Client error)	客户端错误消息	1..1	客户端错误描述
5XX (Server error)	服务器错误消息	1..1	服务器错误描述

> **Note**
>
> 本部分中的示例不包含内容密钥加密。有关如何添加内容密钥加密的信息，请参阅内容密钥加密。

带有明文密钥的实时示例请求负载

以下示例显示加密程序到 DRM 密钥提供程序的典型实时请求负载：

```
<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>
```

带有明文密钥的实时示例响应负载

以下示例显示来自 DRM 密钥提供程序的典型响应负载：

```
<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>
```

SPEKE API v1 - VOD 工作流方法调用示例

请求语法示例

以下 URL 是一个示例，并且不指示固定格式。

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

请求正文

CPIX 元素。

响应标头

名称	类型	发生次数	描述
Speke-User-Agent	字符串	1..1	用于标识密钥提供程序的字符串
Content-Type	字符串	1..1	application/xml

请求响应

HTTP 代码	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 负载响应
4XX (Client error)	客户端错误消息	1..1	客户端错误描述
5XX (Server error)	服务器错误消息	1..1	服务器错误描述

> **Note**
>
> 本部分中的示例不包含内容密钥加密。有关如何添加内容密钥加密的信息，请参阅内容密钥加密。

带有明文密钥的 VOD 示例请求负载

以下示例显示加密程序到 DRM 密钥提供程序的基本 VOD 请求负载：

```
<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>
```

带有明文密钥的 VOD 示例响应负载

以下示例显示来自 DRM 密钥提供程序的基本 VOD 响应负载：

```
<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 - 内容密钥加密

您可以选择将内容密钥加密添加到 SPEKE 实现。内容密钥加密除了对内容本身进行加密外，还通过加密传输的内容密钥来确保全面 end-to-end保护。如果您未为密钥提供程序实现此项，则依靠传输层加密以及强大的身份验证来实现安全性。

要对在 AWS 云中运行的加密器使用内容密钥加密，客户需要将证书导入 AWS Certifice Manager，然后使用生成的证书 ARNs 进行加密活动。加密器使用证书 ARNs 和 ACM 服务向 DRM 密钥提供者提供加密的内容密钥。

限制

SPEKE 支持具有以下限制的 DASH-IF CPIX 规范中指定的内容密钥加密：

- SPEKE 不支持请求或响应负载的数字签名验证（XMLDSIG）。
- SPEKE 需要基于 2048 位 RSA 的证书。

这些限制也在 DASH-IF 规范的自定义项和约束中列出。

实现内容密钥加密

要提供内容密钥加密，请在您的 DRM 密钥提供程序实现中包含以下内容：

- 处理请求和响应负载中的 `<cpix:DeliveryDataList>` 元素。

- 在响应负载的 <cpix:ContentKeyList> 中提供加密值。

有关这些元素的更多信息，请参阅 DASH-IF CPIX 2.0 规范。

请求负载中的示例内容密钥加密元素 <cpix:DeliveryDataList>

下面的示例以粗体突出显示了增加的 <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>
```

响应负载中的示例内容密钥加密元素 <cpix:DeliveryDataList>

下面的示例以粗体突出显示了增加的 <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>
```

响应负载中的示例内容密钥加密元素 <cpix:ContentKeyList>

下面的示例显示了在响应负载的 <cpix:ContentKeyList> 元素中的加密内容密钥处理。这将使用 <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>
```

相比而言，以下示例显示了类似的响应负载，其中包含以未加密的明文密钥形式提供的内容密钥。这将使用 <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 - 检测信号

请求语法示例

以下 URL 是一个示例，并且不指示固定格式：

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

请求响应

HTTP 代码	负载名称	发生次数	描述
200 (Success)	statusMessage	1..1	描述状态的消息

SPEKE API v1 - 覆盖密钥标识符

每轮换一次密钥，加密程序就会创建一个新的密钥标识符 (KID)。它将 KID 传递到其请求中的 DRM 密钥提供程序。通常，使用相同 KID 的密钥提供程序会响应，但它可以在响应中提供其他 KID 值。

以下是 KID 为 11111111-1111-1111-1111-111111111111 的示例请求：

```
   <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>
```

以下响应将 KID 覆盖为 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

这是用于安全打包器和编码器密钥交换 (SPEKE) v2 的 REST API。使用此规范为使用加密的客户提供 DRM 版权保护。为了符合 SPEKE，您的 DRM 密钥提供程序必须公开本规范中描述的 REST API。加密程序对您的密钥提供程序进行 API 调用。

> **Note**
>
> 本规范中的代码示例仅用于说明目的。您无法运行这些示例，因为它们不是完整的 SPEKE 实现的一部分。

SPEKE 使用 DASH 行业论坛内容保护信息交换格式 (DASH-IF-CPIX) 数据结构定义进行密钥交换，但有一些限制。 DASH-IF-CPIX定义了一个架构，以提供从 DRM 平台到加密器的可扩展的多 DRM 交换。这使得在内容压缩和打包时允许对所有自适应比特率打包格式进行内容加密。自适应比特率打包格式包括 HLS、DASH 和 MSS。

从其 2.0 版本开始，SPEKE 与特定的 CPIX 版本保持一致：

在 SPEKE 方面，通过使用 X-Speke-Version HTTP 标头强制执行一致性；在 CPIX 方面，则通过使用 CPIX@version 属性来强制执行一致性。请求中缺少这些元素是 SPEKE v1 传统工作流的典型特征。在 SPEKE v2 工作流中，只有当密钥提供程序同时支持两个版本参数时，它才应处理 CPIX 文档。

有关交换格式的详细信息，请参阅 DASH 行业论坛 CPIX 2.3 规范。

总体而言，与 SPEKE v1.0 相比，SPEKE v2.0 带来了以下演变：

- SPEKE XML 命名空间中的所有标签已弃用，改为使用 CPIX XML 命名空间中的等效标签
- SPEKE:ProtectionHeader 已弃用并替换为 CPIX:DRMSystem.SmoothStreamingProtectionHeaderData
- CPIX:URIExtXKey、SPEKE:KeyFormat 和 SPEKE:KeyFormatVersions 已弃用并替换为 CPIX:DRMSystem.HLSSignalingData
- CPIX@id 替换为 CPIX@contentId
- 新的强制性 CPIX 属性：CPIX@version、ContentKey@commonEncryptionScheme
- 新的可选 CPIX 元素：DRMSystem.ContentProtectionData
- 支持多个内容密钥
- SPEKE 和 CPIX 之间的跨版本控制机制
- HTTP 标头的演变：新的 X-Speke-Version 标头，Speke-User-Agent 标头重命名为 X-Speke-User-Agent
- 检测信号 API 已弃用

由于 SPEKE v1.0 规范保持不变，因此现有实施无需更改即可继续支持 SPEKE v1.0 工作流。

主题

- SPEKE API v2 - 有关 DASH-IF 规范的自定义项和约束
- SPEKE API v2 - 标准负载组件
- SPEKE API v2 - 加密合约

- SPEKE API v2 - 实时工作流方法调用示例
- SPEKE API v2 - VOD 工作流方法调用示例
- SPEKE API v2 - 内容密钥加密
- SPEKE API v2 - 覆盖密钥标识符

SPEKE API v2 - 有关 DASH-IF 规范的自定义项和约束

DASH 行业论坛 CPIX 2.3 规范支持大量使用案例和拓扑。SPEKE API v2.0 规范定义了 CPIX 配置文件和 CPIX 的 API。为了实现这两个目标，它遵循 CPIX 规范，并具有以下自定义项和约束：

CPIX 配置文件

- SPEKE 遵循 Encryptor Consumer 工作流。
- 对于加密的内容密钥，SPEKE 应用以下限制：
  - SPEKE 不支持请求或响应负载的数字签名验证（XMLDSIG）。
  - SPEKE 需要基于 2048 位 RSA 的证书。
- SPEKE 仅利用 CPIX 功能的子集：
  - SPEKE 会忽略 `UpdateHistoryItemList` 功能。如果响应中包含该列表，则 SPEKE 会将其忽略。
  - SPEKE 忽略根/叶密钥功能。如果响应中包含 `ContentKey@dependsOnKey` 属性，则 SPEKE 会将其忽略。
  - SPEKE 会忽略 `BitrateFilter` 元素和 `VideoFilter@wcg` 属性。如果这些元素或属性存在于 CPIX 负载中，SPEKE 会将其忽略。
- 在与 SPEKE v2 交换的 CPIX 文档中，只能使用标准负载组件页面或加密合同页面上提及“支持”的元素或属性。
- 由加密程序包含在 CPIX 请求中时，所有元素和属性都应在密钥提供程序 CPIX 响应中带有有效值。否则，加密程序应停止并引发错误。
- SPEKE 支持使用 `KeyPeriodFilter` 元素进行密钥轮换。SPEKE 仅使用 `ContentKeyPeriod@index` 来跟踪密钥周期。
- 对于 HLS 信令，必须使用多个 `DRMSystem.HLSSignalingData` 元素：一个元素的 `DRMSystem.HLSSignalingData@playlist` 属性值为“media”，另一个元素的 `DRMSystem.HLSSignalingData@playlist` 属性值为“master”。
- 当请求密钥时，加密程序可能会在 `ContentKey` 元素上使用可选的 `@explicitIV` 属性。密钥提供程序可以使用 `@explicitIV` 来响应 IV，即使该属性未包含在请求中。

- 加密程序创建密钥标识符 (KID)，这对于任何给定的内容 ID 和密钥周期保持不变。密钥提供程序在其对请求文档的响应中包含 KID。
- 加密程序应包含 CPIX@contentId 属性的值。当收到此属性的空值时，密钥提供程序应返回一条错误，相应描述为“缺少 CPIX@contentId”。CPIX@contentId 值不能被密钥提供程序覆盖。

  CPIX@id 值（如果不为空）应被密钥提供程序忽略。
- 加密程序应包含 CPIX@version 属性的值。当收到此属性的空值时，密钥提供程序应返回一条错误，相应描述为“缺少 CPIX@version”。收到带有不支持版本的请求时，密钥提供程序返回的错误描述应为“不支持的 CPIX@version”。

  CPIX@version 值不能被密钥提供程序覆盖。
- 加密程序应包括每个所请求密钥的 ContentKey@commonEncryptionScheme 属性值。当收到此属性的空值时，密钥提供者应返回一条错误消息，描述为 “缺少 ContentKey @ commonEncryptionScheme for KIDid”。

  唯一的 CPIX 文档不能混合不同 ContentKey@commonEncryptionScheme 属性的多个值。收到此类组合时，密钥提供者应返回错误信息，并说明为 “不合规 ContentKey @ commonEncryptionScheme 组合”。

  并非所有 ContentKey@commonEncryptionScheme 值都与所有 DRM 技术兼容。收到这样的组合时，密钥提供者应返回一个错误，描述为 “ContentKey@ commonEncryptionScheme 不兼容 DRMSystem id”。

  ContentKey@commonEncryptionScheme 值不能被密钥提供程序覆盖。
- 在 CPIX 响应正文中接收到 DRMSystem@PSSH 和 DRMSystem.ContentProtectionData innerXML <pssh> 元素的不通知时，加密程序应停止并引发错误。

CPIX 的 API

- 密钥提供程序应包含 X-Speke-User-Agent HTTP 响应标头的值。
- 符合 SPEKE 的加密程序充当客户端并向密钥提供程序端点发送 POST 操作。
- 加密器应包含 X-Speke-Version HTTP 请求标头的值，请求中使用的 SPEKE 版本，表述为。MajorVersion MinorVersion，比如 SPEKE v2.0 的 “2.0”。如果密钥提供程序不支持加密程序在当前请求中使用的 SPEKE 版本，则密钥提供程序将返回错误，相应描述为“不支持的 SPEKE 版本”，并且不会尝试尽力处理 CPIX 文档。

  密钥提供程序无法在响应请求时修改加密程序定义的 X-Speke-Version 标头值。

- 在响应正文中收到错误时，加密程序应引发错误，并且不会使用 SPEKE v1.0 版本控制重试请求。

  如果密钥提供程序没有返回错误，但未能返回包含强制信息的 CPIX 文档，则加密程序应停止并引发错误。

下表汇总了消息正文中密钥提供程序必须返回的标准消息。错误情况下的 HTTP 响应代码应为 4XX 或 5XX，绝不会是 200。422 错误代码可用于所有与 SPEKE/CPIX 相关的错误。

错误案例	错误消息
CPIX@contentId 未定义	缺少 CPIX@contentId
CPIX@version 未定义	缺少 CPIX@version
不支持 CPIX@version	不支持的 CPIX@version
ContentKey@ commonEncryptionScheme 未定义	KID 缺少 ContentKey @ commonEncryptionScheme `id`（其中`id`等于 ContentKey @kid 值）
在单个 CPIX 文档中使用多个 ContentKey @ commonEncryptionScheme 值	不合规 ContentKey @ commonEncryptionScheme 组合
ContentKey@ commonEncryptionScheme 与 DRM 技术不兼容	ContentKey@ commonEncryptionScheme 不兼容 DRMSystem `id`（其中`id`等于 DRMSystem @systemId 值）
X-Speke-Version 标头值不是支持的 SPEKE 版本	不支持的 SPEKE 版本
加密合约格式不正确	格式不正确的加密合约
加密合约与 DRM 安全级别约束相矛盾	不支持请求的 CPIX 加密合约
加密合同不包含任何 VideoFilter 或 AudioFilter 元素	缺少 CPIX 加密合约

SPEKE API v2 - 标准负载组件

根据为给定内容定义的加密合约，通过单个 SPEKE 请求，加密程序可以请求多个内容密钥，以及针对多种打包格式的必要清单信令。

为了涵盖所有这些方面，标准的 CPIX 文档由三个强制列表部分组成，外加一个用于实时内容密钥轮换的可选列表部分。

<cpix:CPIX><cpix: ContentKeyList > 分区和顶级元素

这是一个强制部分，与实时和 VOD 流式处理有关，其中定义加密程序需要使用的不同内容密钥。<cpix:ContentKeyList> 元素可以包含一个或多个 <cpix:ContentKey> 子元素，每个子元素都描述一个不同的内容密钥。

根据 CPIX 规范，ContentKey@commonEncryptionScheme 属性的可能值在 ISO 基础媒体文件格式文件通用加密规范（ISO/IEC 23001-7:2016）中定义：

- 'cenc'：AES-CTR 模式完整样本和视频 NAL 子样本加密
- 'cbc1'：AES-CBC 模式完整样本和视频 NAL 子样本加密
- 'cens'：AES-CTR 模式部分视频 NAL 模式加密
- 'cbcs'：AES-CBC 模式部分视频 NAL 模式加密

以下示例显示带有单个非加密内容密钥的 CPIX 文档：

```
<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>
```

默认情况下，内容密钥不加密，如下例所示。但是，加密器可以通过包含<cpix : >元素来请求对内容密钥进行加密。DeliveryDataList有关更多详细信息，请参阅“内容密钥加密”部分。

SPEKE 支持的元素	强制属性	可选属性	强制子元素	可选子元素
<cpix:CPIX>	contentId、version、xmlns:cpix、xmlns:pskc	name、xmlns:enc	一个 <cpix: ContentKeyList >，一个 <cpix : List>，一个 <cpix: DRMSystem > ContentKeyUsageRuleList	一个 <cpix: DeliveryDataList >，一个 <cpix : >ContentKeyPeriodList
<cpix : >ContentKeyList	-	id	至少有一个 <cpix : >ContentKey	-
<cpix : >ContentKey	孩子，commonEncryptionScheme，数据	id、Algorithm、explicitIV	一个 <pskc:Secret>	-
<pskc:Secret>	PlainValue 或者 EncryptedValue	ValueMAC	-	<enc: EncryptionMethod >，<enc : >CipherData

<cpix: 列表> 部分 DRMSystem

这是一个强制部分，与实时和 VOD 流式处理有关，其中定义需要与内容密钥结合利用的不同 DRM 系统。

以下示例显示了包含单个 DRM 系统规格的 PlayReady DRM 系统列表：

```
<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>
```

有关 DRM 系统的完整列表IDs，请参阅 DASH-IF 标识符存储库的 “内容保护” 部分。

SPEKE 支持的元素	强制属性	可选属性	强制子元素	可选子元素
<cpix：列表> DRMSystem	-	id	至少有一个 <cpix : >DRMSystem	-
<cpix : >DRMSystem	kid、systemId	id、name、PSSH	-	ContentProtectionData，SmoothStreamingProtectionHeaderData，两个 <cpix：具有不同播放列表属性值的 HLSSignalingData> 元素

如果将 ISO-BMFF 封装应用于媒体分段，则 DRMSystem@PSSH 为必填项。加密程序仅将 DRMSystem.ContentProtectionData innerXML <pssh> 元素用于清单信令目的。

如果存在 DRMSystem@PSSH 且 DRMSystem.ContentProtectionData 包含 innerXML <pssh> 元素，则两个值应相同。

如果要在 HLS 清单中传送 DRMSystem 信令，则必须在 CPIX 请求和响应中同时包含 <cpix:HLSSignalingData playlist="media"> 和 <cpix:HLSSignalingData playlist="master"> 元素。

<cpix : >部分 ContentKeyPeriodList

这是一个可选部分，仅与实时流式处理有关，它定义了应用于内容的加密周期。

<cpix:ContentKeyPeriodList> 元素可以包含一个或多个 <cpix:ContentKeyPeriod> 子元素，每个子元素都描述了实时时间线中不同的加密周期。 UUIDs 作为 id 属性值的一部分使用是一种常用的方法。

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

SPEKE 支持的元素	强制属性	可选属性	强制子元素	可选子元素
<cpix : >ContentKeyPeriodList	-	id	至少有一个 <cpix : >ContentKeyPeriod	-
<cpix : >ContentKeyPeriod	id、index	-	-	-

如果使用加密周期，则还需要将加密密钥附加到 CPIX 文档中的一个加密周期，如以下部分所示。

<cpix : >部分 ContentKeyUsageRuleList

这是一个强制部分，与实时和 VOD 流式处理有关，定义了不同的内容密钥将如何保护流集内和加密周期的轨道。

<cpix: ContentKeyUsageRuleList > 元素可以包含一个或多个 <cpix: ContentKeyUsageRule > 子元素，每个子元素都描述了加密器可能在特定的加密期间应用给定内容密钥的轨道。<cpix: AudioFilter > 元素中至少需要一个 <cpix: VideoFilter > 或一个<cpix : >元素。ContentKeyUsageRule

以下示例显示了一个简单的列表，其中只有一条规则，将单个内容密钥应用于特定加密周期内的所有音频和视频轨道。

```
<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>
```

SPEKE 支持的元素	强制属性	可选属性	强制子元素	可选子元素
<cpix :>ContentKeyUsageRuleList	-	id	至少有一个 <cpix :>ContentKeyUsageRule	-
<cpix :>ContentKeyUsageRule	孩子，intendedTrackType	-	至少一个 <cpix: AudioFilter > 或者一个 <cpix :>(*) VideoFilter	<cpix :>KeyPeriodFilter
<cpix :>KeyPeriodFilter	periodId	-	-	-
<cpix : >AudioFilter	-	minChannels、maxChannels	-	-
<cpix : >VideoFilter	-	minPixels、maxPixels、hdr、minFps、maxFps	-	-

（*）要详细了解如何使用单个或多个内容密钥来保护流集中的一个或多个轨道，请参阅加密合约文档部分。

SPEKE API v2 - 加密合约

加密合约根据轨道特征定义使用哪些内容密钥来保护给定流集中的哪些轨道。

建议将多个内容密钥用于流集中的不同轨道，但这并不是强制性，而是建议的行业最佳实践 - 至少使用两个不同的内容密钥，一个用于音频轨道，一个用于视频轨道。使用单个内容密钥加密多个轨道是可能的，但需要在加密程序发送给密钥提供程序的 CPIX 文档中明确发出信号。一般而言，加密程序总是准确描述需要多少内容密钥以及如何利用它们来加密各种媒体轨道。

原则

加密合约位于 CPIX 文档的 <cpix:ContentKeyUsageRuleList> 部分。在此部分中，<cpix:ContentKeyList> 部分中定义的每个内容密钥都对应一个特定的 <cpix:ContentKeyUsageRule> 元素，其中应包括：

- 可以引用一个或多个子组件的 ContentKeyUsageRule@intendedTrackType 属性，如果使用多个子组件，则用“+”符号分隔。ContentKeyUsageRule@intendedTrackType 的值在加密合约中应是唯一的，并且不能用于多个 ContentKeyUsageRule 元素。
- 一个或多个 <cpix:AudioFilter> 或 <cpix:VideoFilter> 子元素，具体取决于 ContentKeyUsageRule@intendedTrackType 属性的值。

管理这种关系的规则如下：

- 当需要使用唯一的内容密钥保护流集中的所有音频和视频轨道时，必须使用字符串 'ALL' 作为 ContentKeyUsageRule@intendedTrackType 属性值。示例 1 显示这样的使用案例。在这种情况下，应包括没有任何属性的 <cpix:AudioFilter /> 和 <cpix:VideoFilter /> 子元素。在此特定上下文中，<cpix:AudioFilter> 和/或 <cpix:VideoFilter> 元素的任何其他组合均无效。
- 对于所有其他使用案例，可以自由定义 ContentKeyUsageRule@intendedTrackType 属性的值，并且 <cpix:AudioFilter /> 和 <cpix:VideoFilter /> 子元素的数量必须与通过“+”符号聚合的子组件数量相对应。示例 2/3/4/5/6/7/9/10 说明了当 ContentKeyUsageRule@intendedTrackType 属性值中存在单个子组件时的这一要求。示例 8 说明了使用多个子组件的情况：ContentKeyUsageRule@intendedTrackType="SD+HD" 由两个具有不同属性值的不同 <cpix:VideoFilter> 子元素描

述，ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD" 由三个具有不同属性值的不同 <cpix:VideoFilter> 子元素描述。

筛选条件

CPIX 定义了多个筛选元素和属性，但是 SPEKE 仅支持其中的一个子集。下表对这些不同情况进行了汇总：

CPIX 筛选条件类型	整体 SPEKE 支持	SPEKE 支持的筛选条件属性	SPEKE 不支持的筛选条件属性
<cpix : >VideoFilter	是	minPixels、maxPixels、hdr、minFps、maxFps（可选属性）	wcg
<cpix : >AudioFilter	是	minChannels、maxChannels（可选属性）	
<cpix : >KeyPeriodFilter	是	periodId（强制属性）	
<cpix : >BitrateFilter	否	不适用	不适用
<cpix : >LabelFilter	否	不适用	不适用

根据CPIX的规范 VideoFilter，[minPixels，maxPixels] 是两个维度的全包范围，而（minFPs，maxFPS）仅包含在maxFPS维度上。因为 AudioFilter，[minChannels，MaxChannels] 在两个维度上都是一个包含范围。

问题情况

在某些情况下，加密合约中提供的信息可能不完整、含糊不清或存在错误。在这些情况下，加密程序和密钥提供程序必须采取适当的行为并保证对内容的适当保护。下表列出了在这些情况下的建议行为：

在这种情况下	加密程序器应该...	密钥提供程序应该...
没有规则适用于流集中的一个或多个轨道（参见下面的示例 3）	加密程序应查看其配置（CPIX 负载外部），并验证相关轨道是否不需要加密。如果不是预期情况，则加密程序应引发错误并停止处理。	不相关：密钥提供程序不了解流集结构。
多个规则重叠并建议使用多个内容密钥来加密特定轨道	加密器应按文档顺序应用最后一次 ContentKeyUsageRule 成功评估的结果。	不相关：密钥提供程序不了解流集结构。
加密合约在单个 SPEKE 请求/响应周期中更改	加密程序应引发异常并停止处理，因为密钥提供程序不负责定义加密合约。	为了防止这种情况发生，密钥提供程序不得修改在 SPEKE 请求的 CPIX 负载中收到的加密合约。
格式错误的加密合约：intendedTrackType/Filters 基数约束异常、不支持的过滤器或属性	加密器程序引发异常，停止处理，并且不向密钥提供程序发送 SPEKE 请求，因为这很可能会导致错误的内容保护或使某些轨道不受保护。	密钥提供程序应引发异常并返回“格式错误的加密合约”错误。
格式良好的加密合约，但违反了 DRM 安全级别的约束：例如，要求使用单个内容密钥来保护音频轨道和超高清视频轨道	如果加密程序了解 DRM 安全级别约束，则应引发异常，停止处理，不向密钥提供程序发送 SPEKE 请求，因为这很可能会导致错误的内容保护。	密钥提供程序应引发异常并返回“不支持请求的 CPIX 加密合约”错误。
缺少加密合约	加密器不得发送不包含任何或 VideoFilter 元素的CPIX文档。AudioFilter	密钥提供程序应引发异常并返回“缺少 CPIX 加密合约”错误。

加密合约示例

示例 1：所有音频和视频轨道都使用一个内容密钥

```
<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>
```

示例 2：一个内容密钥用于所有视频轨道，一个内容密钥用于所有音频轨道

```
<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>
```

示例 3：一个内容密钥用于所有视频轨道和未加密的音频轨道

```
<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>
```

示例 4：多个内容密钥用于不同的视频轨道（SD/HD），一个内容密钥用于所有音频轨道

```
<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>
```

示例 5：多个内容键用于不同的视频轨道 (SD/HD/UHD)，一个内容键用于所有音轨

```
<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>
```

示例 6：多个内容键用于不同的视频轨道 (SD/HD/UHD1/UHD2)，一个内容键用于所有音轨

```
<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>
```

示例 7：不同的视频轨道有多个内容键 (SD/HD1/HD2/UHD1/UHD2)，一个内容键用于所有音轨

```
<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>
```

示例 8：多个内容密钥用于不同的视频轨道（基于多个属性类型），一个内容密钥用于所有音频轨道

```
<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>
```

示例 9：一个内容密钥用于所有视频轨道，多个内容密钥用于立体声和多声道音频轨道

```
<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>
```

示例 10：一个内容密钥用于所有视频轨道，多个内容密钥用于立体声和两种类型的多声道音频轨道

```
<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 - 实时工作流方法调用示例

请求语法示例

以下 URL 是一个示例，并且不指示固定格式：

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

请求正文

CPIX 文档。

请求标头

名称	类型	发生次数	描述
AWS Authorization	字符串	1..1	请参阅 AWS Sigv4
X-Amz-Security-Token	字符串	1..1	请参阅 AWS Sigv4
X-Amz-Date	字符串	1..1	请参阅 AWS Sigv4
Content-Type	字符串	1..1	application/xml
X-Speke-Version	字符串	1..1	与请求一起使用的 SPEKE API 版本，公式为。 MajorVersion MinorVersion，比如 SPEKE v2.0 的 “2.0”

响应标头

名称	类型	发生次数	描述
X-Speke-User-Agent	字符串	1..1	用于标识密钥提供程序的字符串
Content-Type	字符串	1..1	application/xml
X-Speke-Version	字符串	1..1	与请求一起使用的 SPEKE API 版本，公式为。 MajorVersion MinorVersion，比如 SPEKE v2.0 的 “2.0”

请求响应

HTTP 代码	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 负载响应
4XX (Client error)	客户端错误消息	1..1	客户端错误描述
5XX (Server error)	服务器错误消息	1..1	服务器错误描述

> **Note**
>
> 本部分中的示例不包含内容密钥加密。有关如何添加内容密钥加密的信息，请参阅内容密钥加密。

带有明文密钥的实时示例请求负载

以下示例显示了从加密程序到 DRM 密钥提供程序的典型实时请求负载，一个内容密钥用于所有视频轨道，一个内容密钥用于所有音频轨道：

```
<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>
```

带有明文密钥的实时示例响应负载

以下示例显示了来自 DRM 密钥提供程序的典型响应负载（为了便于阅读，返回值已使用 [...] 缩短）：

```
<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 工作流方法调用示例

请求语法示例

以下 URL 是一个示例，并且不指示固定格式。

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

请求正文

CPIX 文档。

请求标头

名称	类型	发生次数	描述
AWS Authorization	字符串	1..1	请参阅 AWS Sigv4
X-Amz-Security-Token	字符串	1..1	请参阅 AWS Sigv4
X-Amz-Date	字符串	1..1	请参阅 AWS Sigv4
Content-Type	字符串	1..1	application/xml
X-Speke-Version	字符串	1..1	与请求一起使用的 SPEKE API 版本，公式为。 MajorVersion

名称	类型	发生次数	描述
			MinorVersion，比如 SPEKE v2.0 的 “2.0”

响应标头

名称	类型	发生次数	描述
`X-Speke-User-Agent`	字符串	1..1	用于标识密钥提供程序的字符串
`Content-Type`	字符串	1..1	application/xml
`X-Speke-Version`	字符串	1..1	与请求一起使用的 SPEKE API 版本，公式为。 MajorVersion MinorVersion，比如 SPEKE v2.0 的 “2.0”

请求响应

HTTP 代码	负载名称	发生次数	描述
`200 (Success)`	CPIX	1..1	DASH-CPIX 负载响应
`4XX (Client error)`	客户端错误消息	1..1	客户端错误描述
`5XX (Server error)`	服务器错误消息	1..1	服务器错误描述

> **Note**
>
> 本部分中的示例不包含内容密钥加密。有关如何添加内容密钥加密的信息，请参阅内容密钥加密。

带有明文密钥的 VOD 示例请求负载

以下示例显示了从加密程序到 DRM 密钥提供程序的典型 VOD 请求负载，一个内容密钥用于所有视频轨道，一个内容密钥用于所有音频轨道：

```
<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>
```

带有明文密钥的 VOD 示例响应负载

以下示例显示了来自 DRM 密钥提供程序的典型响应负载（为了便于阅读，返回值已使用 [...] 缩短）：

```
<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 - 内容密钥加密

您可以选择将内容密钥加密添加到 SPEKE 实现。内容密钥加密除了对内容本身进行加密外，还通过加密传输的内容密钥来确保全面 end-to-end保护。如果您未为密钥提供程序实现此项，则依靠传输层加密以及强大的身份验证来实现安全性。

要对在 AWS 云中运行的加密器使用内容密钥加密，客户需要将证书导入 AWS Certifice Manager，然后使用生成的证书 ARNs 进行加密活动。加密器使用证书 ARNs 和 ACM 服务向 DRM 密钥提供者提供加密的内容密钥。

限制

SPEKE 支持具有以下限制的 DASH-IF CPIX 规范中指定的内容密钥加密：

- SPEKE 不支持请求或响应负载的数字签名验证（XMLDSIG）。
- SPEKE 需要基于 2048 位 RSA 的证书。

这些限制也在 DASH-IF 规范的自定义项和约束中列出。

实现内容密钥加密

要提供内容密钥加密，请在您的 DRM 密钥提供程序实现中包含以下内容：

- 处理请求和响应负载中的 <cpix:DeliveryDataList> 元素。
- 在响应负载的 <cpix:ContentKeyList> 中提供加密值。

有关这些元素的更多信息，请参阅 DASH-IF CPIX 2.3 规范。

请求负载中的示例内容密钥加密元素 <cpix:DeliveryDataList>

```
<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>
```

响应负载中的示例内容密钥加密元素 <cpix:DeliveryDataList>

```
<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>
```

响应负载中的示例内容密钥加密元素 `<cpix:ContentKeyList>`

下面的示例显示了在响应负载的 <cpix:ContentKeyList> 元素中的加密内容密钥处理。这将使用 <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>
```

相比而言，以下示例显示了类似的响应负载，其中包含以未加密的明文密钥形式提供的内容密钥。这将使用 <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 - 覆盖密钥标识符

每轮换一次密钥，加密程序就会创建一个新的密钥标识符 (KID)。它将 KID 传递到其请求中的 DRM 密钥提供程序。通常，使用相同 KID 的密钥提供程序会响应，但它可以在响应中提供其他 KID 值。

以下是 KID 为 11111111-1111-1111-1111-111111111111 的示例请求：

```
<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>
```

以下响应将 KID 覆盖为 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 规范的许可证

知识共享署名-ShareAlike 4.0 国际公共许可

行使许可权（定义见下文），即表示您接受并同意受本知识共享署名-ShareAlike 4.0国际公共许可（“公共许可”）的条款和条件的约束。鉴于本公共许可证可以被解释为合同，在您接受这些条款和条件的前提下，将为您授予许可权利；在许可人根据这些条款和条件从提供许可材料中获益的前提下，许可人为您授予这些权利。

第 1 条 – 定义。

a. “演绎材料”是指受著作权和类似权利限制的材料，它来源于或基于许可材料，并以某种方式翻译、改动、编排和转换许可材料或以其他方式修改许可材料而需要根据许可人拥有的著作权和类似权利进行许可。对于本公共许可证而言，当许可材料为音乐作品、表演或录音时，将许可材料依时间序列关系与动态影像配合一致而形成的结果，视为演绎材料。

b. “演绎者的许可证”是指，您根据本公共许可证的条款和条件为针对演绎材料所做的工作申请的著作权和类似权利。

c. BY-SA 兼容许可证是指在 creativecommons.org/compatiblelicenses 上列出的许可证，该许可证经知识共享批准，基本上等同于本公共许可证。

d. “著作权和类似权利”是指著作权和/或与著作权密切相关的类似权利，包括但不限于表演、广播、录音以及独特数据库权利，而与如何对这些权利进行标记或分类无关。就本公共许可证而言，第 2(b)(1)-(2) 条中规定的权利不是著作权和类似权利。

e. “有效技术措施”是指，在没有正确授权的情况下，根据 1996 年 12 月 20 日制订的 WIPO 著作权公约第 11 条和/或类似的国际协议履行的法律义务，不得规避这些措施。

f. “例外和限制”是指，对适用于您使用许可材料的著作权和类似权利的合理使用、公平交易和/或任何其他例外或限制。

g. 许可证元素是指知识共享公共许可证名称中列出的许可证属性。本公共许可证的许可要素是署名和 ShareAlike.

h. “许可材料”是指，许可人将本公共许可证应用到的艺术或文学作品、数据库或其他材料。

i. “许可权利”是指根据本公共许可证的条款和条件为您授予的权利，这些权利仅限于适用于您使用许可材料的所有著作权和类似权利以及许可人有权许可的著作权和类似权利。

j. “许可人”是指根据本公共许可证向其授予权利的个人或实体。

k. “共享”是指以任何方式或程序（如复制、公开展示、公开表演、发行、分发、传播或进口）向公众提供材料需要根据许可权利获得许可，包括以特定方式向公众提供材料，以使公众成员可以在自己单独选择的地点和时间获得这些材料。

l. “独特数据库权利”是指，1996 年 3 月 11 日欧洲议会和理事会制订的关于数据库法律保护的指令 96/9/EC（作为修订或替代版本）规定的著作权以外的权利以及世界上任何地方的其他基本相同的权利。

m. “您”是指根据本公共许可证行使许可权利的个人或实体。“您的”具有相应的含义。

第 2 条 – 范围。

a. 授权。

1. 根据本公共许可证的条款和条件，许可人特此授予您全球性、免版税、不得再授权、非独占、不可撤销的许可证，以便行许可材料的许可权利以完成以下操作：

A. 全部或部分复制和共享许可材料；以及

B. 制作、复制和共享演绎材料。

2. 例外和限制。为避免疑义，如果例外和限制适用于您的使用，则本公共许可证不适用，您不需要遵守其条款和条件。
3. 期限。第 6(a) 条规定了本公共许可证的期限。
4. 媒体和格式；允许技术修改。许可人授权您在所有媒体和格式 (无论是现在已知还是以后创建的) 中行使许可权利，并根据需要进行技术修改。许可人放弃和/或同意不主张任何权利或权限以禁止您进行所需的技术修改以行使许可权利，包括为规避有效技术措施所需的技术修改。就本公共许可证而言，仅进行第 2(a)(4) 条授权的修改不会被视为演绎材料。
5. 下游接收人。
   A. 许可人提供的授权 - 许可材料。许可材料的每个接收人自动获得许可人提供的授权，以便根据本公共许可证的条款和条件行使许可权利。
   B. 许可人额外提供的条件 – 演绎材料。您提供的演绎材料的每位接收方都会自动收到许可人提供的条件，以根据您申请的演绎者许可证条件行使演绎材料的许可权利。
   C. 没有下游限制。您不得向许可材料提供或施加任何额外或不同的条款或条件或应用任何有效技术措施，如果这样做，将会限制任何许可材料接收人行使许可权利。
6. 未认可。本公共许可证中的任何内容均不构成或可以解释为允许声明或暗示您或您使用许可材料与许可人或指定的其他人有关联，或者赞助、认可或授予官方身份以获得第 3(a)(1)(A)(i) 条规定的署名。

b. 其他权利。

1. 道德权利，例如诚信权，未根据本公共许可证获得许可，也未and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or同意在允许您行使许可权利所需的有限范围内主张许可方持有的任何此类权利，但不以其他方式行使。
2. 未依照本公共许可证授予专利和商标权利。
3. 在可能的范围内，许可人放弃因您行使许可权利而向您收取许可使用费的任何权利，无论是直接收取，还是根据任何自愿或可放弃的法定或强制许可方案通过收取协会收取。在所有其他情况下，许可人明确保留收取此类许可使用费的任何权利。

第 3 条 – 许可证条件。

要行使许可权利，您必须明确遵守以下条件。

a. 署名。

1. 如果您共享许可材料（包括修改的形式），您必须：
   A. 如果是许可人随许可材料提供的，则保留以下内容：

```
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. 表明您是否修改了许可材料并保留任何以前修改的说明；以及

C. 表明许可材料是根据本公共许可证许可的，并包括本公共许可证的文本或者 URI 或超链接。

2. 您可以根据共享许可材料的媒体、方式和上下文，以任何合理的方式满足第 3(a)(1) 条中的条件。例如，可以提供包含所需信息的资源的 URI 或超链接以合理地满足这些条件。
3. 如果许可人要求，您必须在切实可行的范围内删除第 3(a)(1)(A) 条要求的任何信息。

b. ShareAlike。 除了第 3 (a) 节中的条件外，如果您共享自己制作的改编材料，则以下条件也适用。

1. 您申请的演绎者许可证必须是具有相同许可证元素的知识共享许可证（此版本或更高版本），或者是 BY-SA 兼容许可证。
2. 您必须附上所申请演绎者许可证的文本、URI 或超链接。您可以根据共享演绎材料的媒体、方式和上下文，以任何合理的方式满足此条件。
3. 您不得对演绎材料提供或强加任何额外或不同的条款或条件，也不得对演绎材料适用任何有效的技术措施，以限制行使您申请的演绎者许可证所授予的权利。

第 4 条 – 独特数据库权利。

如果许可权利包括适用于您使用许可材料的独特数据库权利：

a. 为避免疑义，第 2(a)(1) 条授予您提取、重用、复制和共享全部或大部分数据库内容的权利；

b. 如果将全部或大部分数据库内容包含在您具有独特数据库权利的数据库中，则您具有独特数据库权利的数据库 (而不是其单独内容) 是演绎材料，包括出于第 3(b) 节的目的；以及

c. 如果共享全部或大部分数据库内容，您必须遵守第 3(a) 条中的条件。为避免疑义，如果许可权利包括其他著作权和类似权利，第 4 条将补充而不是替代本公共许可证规定的您的义务。

第 5 条 – 免责声明和责任限制。

a. 除非许可人另行承诺，许可人在可能的范围内按“原样”和可用性提供许可材料，不提供有关许可材料的任何声明或担保，无论是明示的、暗示的、法定的还是其他声明或担保。这包括但不限于所有权、适销性、针对特殊用途的适用性、非侵权、不存在潜在或其他缺陷、准确性或存在或不存在错误 (无论是否已知或可发现) 的担保。如果不允许全部或部分免责声明，则本免责声明可能不适用于您。

b. 在可能的范围内，许可人在任何情况下都不会依据任何法律理论（包括但不限于疏忽）或其他情况对您因本公共许可证或使用许可材料而产生的任何直接、特殊、间接、偶发、继发性、惩罚性、惩戒性或其他损失、费用、开支或损害赔偿负责，即使许可人已被告知发生此类损失、费用、开支或损害的可能性。如果不允许限制全部或部分责任，则本责任限制可能不适用于您。

c. 应以某种方式解释上面提供的免责声明和责任限制，以便在可能的范围内最接近所有责任的绝对免责声明和放弃。

第 6 条 – 期限和终止。

a. 本公共许可证适用于此处授予的著作权和类似权利的期限。不过，如果您未遵守本公共许可证，根据本公共许可证为您授予的权利将自动终止。

b. 如果已根据第 6(a) 条终止您使用许可材料的权利，可以在以下情况下恢复该权利：

   1. 自纠正违规情况之日起自动恢复，但前提是在发现违规之日起 30 日内纠正；或者

   2. 许可人明确恢复该权利。

c. 为避免疑义，第 6(b) 条不影响许可人为您违反本公共许可证而寻求补偿的任何权利。

d. 为避免疑义，许可人也可以根据单独的条款或条件提供许可材料，或者随时停止分发许可材料；不过，这样做不会终止本公共许可证。

e. 即使终止了本公共许可证，第 1 条、第 5 条、第 6 条、第 7 条以及第 8 条仍然有效。

第 7 条 – 其他条款和条件。

a. 除非明确同意，许可人不应受您提出的任何其他或不同的条款或条件的约束。

b. 此处未提及的有关许可材料的任何约定、谅解或协议是与本公共许可证的条款和条件分开的。

第 8 条 – 解释。

a. 为避免疑义，本公共许可证不会也不应被解释为对使用根据本公共许可证合法提供的许可材料减少、限制、限定或施加条件。

b. 在可能的范围内，如果本公共许可证的任何条款被视为不可履行，则会在所需的最低限度内自动修改以使其可履行。如果无法修改该条款，应将其从本公共许可证中删除，而不会影响履行其余条款和条件。

c. 除非许可人明确同意，否则，不会放弃本公共许可证的任何条款或条件，也不会同意不遵守这些条款或条件。

d. 本公共许可证中的任何内容均不构成或可能被解释为限制或放弃适用于许可人或您的任何权利和豁免权，包括来自任何司法管辖区或授权机构的法律程序。

SPEKE 合作伙伴和客户指南的文档历史记录

下表介绍对 SPEKE 文档的一些更改。

SPEKE v1

更改	描述	日期
Support 矩阵：AWS 合作伙伴服务和产品	添加了 AWS 合作伙伴服务和产品中的 SPEKE 支持的新部分，并且列出了 Bitmovin 服务。	2023 年 1 月 13 日
DRM 平台提供商的更新	在 DRM 平台提供商列表中添加链接和新的合作伙伴信息。	2019 年 1 月 24 日
包括第三方加密程序	更新了架构和描述以考虑第三方加密程序。	2018 年 11 月 20 日
内容密钥加密	增加了用于加密内容密钥的选项。在此之前，安全包装程序和编码器密钥交换仅支持清除密钥交付。	2018 年 10 月 30 日
支持矩阵 - AWS Elemental Live	添加 AWS Elemental Live 支持矩阵。	2018 年 9 月 27 日
标准负载组件	增加了一个定义 JSON 负载中的主要元素的部分。	2018 年 9 月 27 日
KID 覆盖	增加了一个有关密钥提供程序覆盖 KID 的部分。	2018 年 9 月 27 日
更正了指向 DASH-IF 站点的链接	更正了 CPIX 规范和系统 IDs 页面的 DASH IF 网站链接。	2018 年 9 月 27 日
发布 AWS Elemental Live 的副本	已更新 SPEKE 文档以包含 AWS Elemental 产品。	2018 年 7 月 20 日

更改	描述	日期
CMAF	已更新服务的支持矩阵表以包括通用媒体应用程序格式（CMAF）。	2018 年 6 月 27 日
初始版本	安全包装程序和编码器密钥交换（SPEKE）版本 1（内容加密程序和 DRM 密钥提供程序之间的通信规范）的首次发布。DRM 密钥提供程序公开安全包装程序和编码器密钥交换 API 来处理传入的密钥请求。	2017 年 11 月 27 日

SPEKE v2

更改	描述	日期
DRM 平台提供商部分以及支持 SPEKE 的 AWS 服务和产品部分的更新	将 Webstream 添加到 DRM 平台提供商列表的 SPEKE v2 列中，已添加 MediaConvert 到 AWS 服务和产品表中 SPEKE 支持表的 SPEKE v2 列中。	2024 年 10 月 10 日
更新 DRM 平台提供商部分	在 DRM 平台提供商列表的 SPEKE v2 列中添加新的合格合作伙伴。	2023 年 8 月 9 日
更新实时和 VOD 工作流方法调用示例部分	在 SPEKE v2 Live 和 VOD 工作流程方法调用示例部分中添加了缺少的 X-Speke-Version 响应标头。	2023 年 1 月 13 日
更新 DRM 平台提供商和加密合约部分	在 DRM 平台提供商列表的 SPEKE v2 列中添加新的合格合作伙伴。添加两个新的加密合约示例，并在所有相关示	2022 年 1 月 27 日

更改	描述	日期
	例中将 SD 最大分辨率更改为 1024x576。	
初始版本	安全包装程序和编码器密钥交换（SPEKE）版本 2.0（内容加密程序和 DRM 密钥提供程序之间的通信规范）的首次发布。DRM 密钥提供程序公开安全包装程序和编码器密钥交换 API 来处理传入的密钥请求。	2021 年 9 月 7 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。