合作伙伴和客户指南

安全打包器和编码器密钥交换API规范

安全打包器和编码器密钥交换API规范: 合作伙伴和客户指南

Table of Contents

什么是安全包装程序和编码器密钥交换？ 1
常规架构 1
AWS基于云的架构 1
如何开始 2
您是首次使用 SPEKE 吗？ 4
相关服务信息和规格 4
术语 4
客户登记 6
开始从DRM平台提供商那里开始 6
SPEKEAWS服务和产品支持 7
SPEKE为AWS合作伙伴服务和产品提供支持 8
SPEKEAPI规格 9
需要进行身份验证 SPEKE 10
AWS云端实施的身份验证 10
本地产品的身份验证 11
SPEKEAPIv1 11
SPEKEAPIv1--IF 规范的自定义和约束 DASH 12
SPEKEAPIv1-标准有效载荷组件 13
SPEKEAPIv1-实时工作流程方法调用示例 15
SPEKEAPIv1-VOD 工作流程方法调用示例 19
SPEKEAPIv1-内容密钥加密 23
SPEKEAPIv1-Heartbeat 26
SPEKEAPIv1-覆盖密钥标识符 27
SPEKEAPIv2 28
SPEKEAPIv2--IF 规范的自定义和约束 DASH 30
SPEKEAPIv2-标准有效载荷组件 33
SPEKEAPIv2-加密合约 37
SPEKEAPIv2-实时工作流程方法调用示例 46
SPEKEAPIv2-VOD 工作流程方法调用示例 52
SPEKEAPIv2-内容密钥加密 57
SPEKEAPIv2-覆盖密钥标识符 60
该SPEKEAPI规范的许可证 62
知识共享署名-ShareAlike 4.0 国际公共许可 62
文档历史记录 68

..... lxxi

什么是安全包装程序和编码器密钥交换？

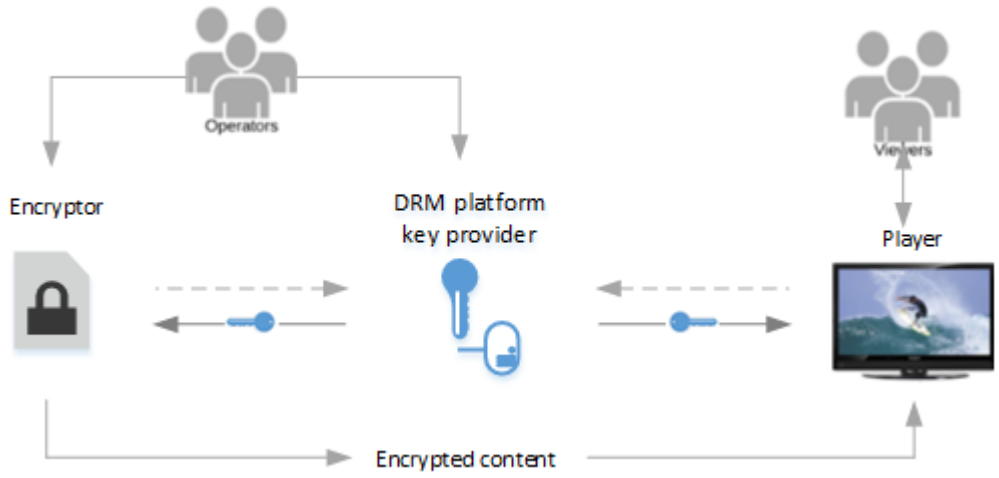
Secure Packager 和 Encoder Key Exchange (SPEKE) 定义了媒体内容的加密者和打包者以及数字版权管理 (DRM) 密钥提供商之间的通信标准。该规范适用于在本地和云端运行的AWS加密器。

主题

- 常规架构
- AWS基于云的架构
- 如何开始

常规架构

下图显示了本地产品的SPEKE内容加密架构的高级视图。

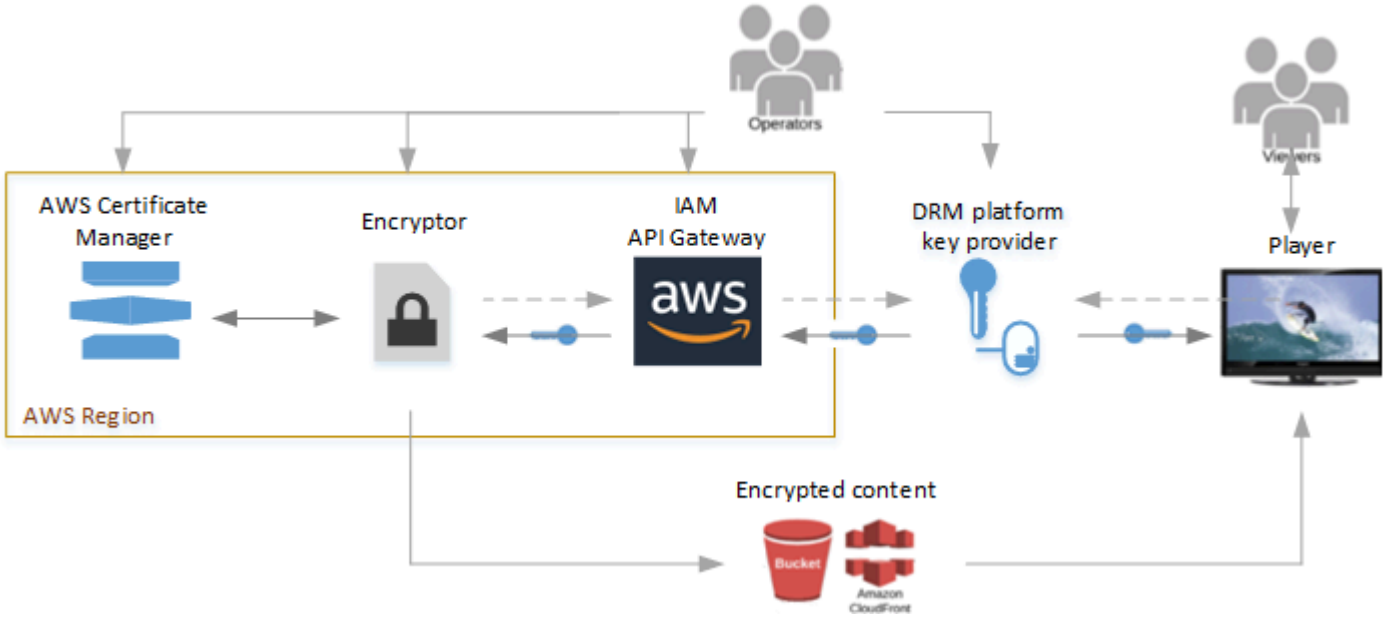


以下是上述架构的主要组件：

- 加密程序 – 提供加密技术。接收来自其运营商的加密请求，并从密钥提供者那里检索所需的密DRM钥以保护加密内容。
- DRM平台密钥提供程序-通过兼容的向加密器提供加密SPEKE密API钥。此外，提供程序将许可证提供给媒体播放器以进行解密。
- Player — 向同一个DRM平台密钥提供者请求密钥，玩家使用密钥来解锁内容并将其提供给观众。

AWS基于云的架构

下图显示了与AWS云中运行的服务和功能一起使用时的SPEKE高级架构。



以下是主要服务和组件：

- 加密器-在AWS云端提供加密技术。加密器接收来自其运营商的请求，并通过 Amazon Gate API way 从密DRM钥提供者那里检索所需的加密密钥，以保护加密内容。它将加密的内容传输到 Amazon S3 存储桶或通过亚马逊 CloudFront 分发传输。
- AWSIAM和 Amazon API Gatewa y — 管理客户信任的角色以及加密器和密钥提供者之间的代理通信。APIGateway 提供日志记录功能，允许客户控制他们与加密器DRM和平台的关系。客户通过IAM角色配置启用密钥提供商访问权限。API网关必须与加密器位于同一个AWS区域。
- AWSCertifice Manager —（可选）为内容密钥加密提供证书管理。要确保通信安全，建议的做法是加密内容密钥。证书管理器必须与加密器位于同一个AWS区域。
- DRM平台密钥提供程序-通过兼容的向加密器提供加密SPEKE密API钥。此外，提供程序将许可证提供给媒体播放器以进行解密。
- Player — 向同一个DRM平台密钥提供者请求密钥，玩家使用密钥来解锁内容并将其提供给观众。

如何开始

有关其他介绍性材料SPEKE，请参阅你是新手SPEKE吗？ 。

您是客户吗？

与 E AWS lemental DRM 平台提供商合作，设置使用加密。有关详细信息，请参阅客户登记。

您是DRM平台提供商还是拥有自己的密钥提供商的客户？

根据SPEKE规范RESTAPI为您的密钥提供商公开一个。有关详细信息，请参阅SPEKEAPI规范。

您是首次使用 SPEKE 吗？

本节为不熟悉 Secure Packager 和 Encoder Key Exchange (SPEKE) 的读者提供入门信息。

有关简介SPEKE，请观看以下网络直播：

相关服务信息和规格

- API网关权限 — 如何使用 Identity and Acces API s Managem AWS ent (AWSIAM) 权限控制对的访问。
- AWS AssumeRole— 如何使用AWS安全令牌服务 (AWSSTS) 来承担角色功能。
- AWSSigv4 — 如何使用签名版本 4 签署HTTP请求。
- DASH-IF CPIX 规范 v2.0 — 本 SPEKE v1.0 规范所基于的 DASH-IF 内容保护信息交换格式 (CPIX) 规范版本。
- DASH-IF CPIX 规范 v2.3 — 本版本 2. SPEKE 0 规范所基于的 DASH-IF 内容保护信息交换格式 (CPIX) 规范版本。
- DASH-IF 系统 IDs-系统的注册标识符列表。DRM
- https://github.com/awslabs/speke-reference-server— 示例参考密钥提供程序，可与您的AWS账户一起使用，以帮助您开始在中SPEKE实施AWS。

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— 亚马逊资源名称。唯一标识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— 数字版权管理。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 — 一种为内容加密者和查看者提供DRM功能和支持的系统，包括为内容加密和解DRM密提供密钥和许可。

- DRM提供商 — 参见DRM平台。
- DRM系统-DRM 实现标准。常见的DRM系统包括苹果 FairPlay、谷歌 Widevine 和微软。PlayReadyDRM系统由内容提供商用来保护数字内容，以便交付给观众和供观众访问。有关使用-IF 注册的DRM系统的列表，请参阅 DASH DASH-IF 系统。IDsDASH-IF CPIX 规范使用此处定义的“DRM系统”一词，在某些地方，它使用 “DRM系统” 来表示本规范所指的DRM平台。
- DRM解决方案-参见DRM平台。
- DRM技术-参见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。加密器通常还会向DRM媒体添加加密信号和元数据。加密程序通常是编码器、包装程序和转码器。
- 密钥提供者-DRM 平台中SPEKERESTAPI用于处理密钥请求的组件。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-维护内容加密和解密密钥的DRM平台组件。
- 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。从不同的来源获取其信息，包括媒体清单文件、媒体文件和DRM许可证。代表观众向DRM平台申请许可证。

的客户入职培训 SPEKE

通过将 Secure Packager 和 Encoder Key Exchange (SPEKE) 数字版权管理 (DRM) 密钥提供程序与您的加密器和媒体播放器相结合，保护您的内容免遭未经授权的使用。SPEKE定义了媒体内容加密者和打包商以及数字版权管理 (DRM) 密钥提供商之间的通信标准。要加入，您需要选择DRM平台密钥提供商并配置密钥提供商与您的加密器和播放器之间的通信。

主题

- 开始从DRM平台提供商那里开始
- SPEKEAWS服务和产品支持
- SPEKE为AWS合作伙伴服务和产品提供支持

开始从DRM平台提供商那里开始

以下 Amazon 合作伙伴为其提供第三方DRM平台实施SPEKE。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	SPEKEv1 支持	SPEKEv2 支持
Axinom	√	√
买 DRM	√	√
castLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKA网络	√	√
Insys 云 DRM	√	√
Intertrust Technologies	√	√

DRM平台提供商	SPEKEv1 支持	SPEKEv2 支持
Irdeto	√	√
JW 播放器	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	√

SPEKEAWS服务和产品支持

本节列出了在AWS云端运行的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器。确认您的流媒体协议和所需的DRM系统可用于您的服务或产品。

AWS服务或产品	SPEKEv1 支持	SPEKEv2 支持	支持的DRM技术
AWSElemental MediaConvert -在云端运行的AWS服务	√	√	文档
AWSElemental MediaPackage -在云端运行的AWS服务	√	√	文档
AWSElemental Live-本地产品	√		文档：MPEG-DASH /HLS

AWS服务或产品	SPEKEv1 支持	SPEKEv2 支持	支持的DRM技术
AWSElemental Server-本地产品	√		文档

SPEKE为AWS合作伙伴服务和产品提供支持

本节列出了在AWS云端运行的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器。确认您的流媒体协议和所需的DRM系统可用于您的服务或产品。

AWS服务或产品	SPEKEv1 支持	SPEKEv2 支持	支持的DRM技术
Bitmovin 实时视频编码	√		文档
Bitmovin 视频点播 () 编码 VOD	√		文档

SPEKEAPI规格

这是安全打包程序和编码器密钥交换 (SPEKE) 的RESTAPI规范。使用本规范为使用加密的客户提供DRM版权保护。

在视频流工作流程中，加密引擎与DRM平台密钥提供者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，当需要进行内容加密时，DRM供应商和客户可以使用该接口与加密器集成。
- 涵盖VOD和实时工作流程，包括加密器和DRM密钥提供商端点之间进行强大、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 Widev CENC ine/。
- 保持规范的简单性和可扩展性，以支持 future DRM 系统。
- 使用简单的 RESTAPI.

> **Note**
>
>

主题

- 需要进行身份验证 SPEKE

- SPEKEAPIv1
- SPEKEAPIv2
- 该SPEKEAPI规范的许可证

需要进行身份验证 SPEKE

SPEKE需要对本地产品以及AWS云端运行的服务和功能进行身份验证。

主题

- AWS云端实施的身份验证
- 本地产品的身份验证

AWS云端实施的身份验证

SPEKE需要通过IAM角色进行AWS身份验证才能与加密器一起使用。IAM角色由DRM提供者或在AWS账户中拥有DRM终端节点的操作员创建。为每个角色分配一个 Amazon 资源名称 (ARN)，AWSElemental 服务操作员在请求加密时在服务控制台上提供该名称。必须将角色的策略权限配置为授予访问密钥提供程序的权限，API而不允许访问其他AWS资源。当加密器联系DRM密钥提供者时，它会使用该角色ARN来扮演密钥提供者账户持有者的角色，后者会返回临时证书，供加密者用来访问密钥提供程序。

一种常见的实现方式是运营商或DRM平台供应商在密钥提供商面前使用 Amazon API Gateway，然后在网API关资源上启用 Ident AWS ity and Access Management (AWSIAM) 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。在本例中，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。

以下示例显示了为访问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。有关签署请求的更多信息，请参阅AWSSigv4。

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，但至少应使用基本身份验证HTTPS。

两种类型的身份验证都使用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身份验证的信息，包括有关标头的详细信息，请参阅 Internet 工程任务组 (IETF) 规范 RFC2617-HTTP 身份验证：基本和摘要访问身份验证。

SPEKEAPIv1

这是 Secure Packager 和 Encoder 密钥交换 (SPEKE) v1 的。REST API使用本规范为使用加密的客户提供DRM版权保护。为了SPEKE符合要求，您的DRM密钥提供程序必须公开本规范中RESTAPI描述的。加密器会API调用您的密钥提供商。

> **Note**
>
> 本规范中的代码示例仅用于说明目的。你无法运行这些示例，因为它们不是完整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重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HLSDASH、和。MSS

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

主题

- SPEKEAPIv1--IF 规范的自定义和约束 DASH
- SPEKEAPIv1-标准有效载荷组件
- SPEKEAPIv1-实时工作流程方法调用示例
- SPEKEAPIv1-VOD 工作流程方法调用示例
- SPEKEAPIv1-内容密钥加密
- SPEKEAPIv1-Heartbeat
- SPEKEAPIv1-覆盖密钥标识符

SPEKEAPIv1--IF 规范的自定义和约束 DASH

DASH-IF CPIX 规范 https://dashif.org/docs/ DASH-IF-CPIX-v2-0.pdf 支持多种用例和拓扑。该SPEKEAPI规范符合规CPIX范，但有以下自定义和约束：

- 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RSA基于 2048 的证书。
- 对于轮换密钥工作流程，SPEKE需要`ContentKeyUsageRule`筛选器`KeyPeriodFilter`。SPEKE忽略所有其他`ContentKeyUsageRule`设置。
- SPEKE 会忽略 `UpdateHistoryItemList` 功能。如果响应中存在该列表，则将其SPEKE忽略。
- SPEKE支持密钥轮换。SPEKE仅使用 `ContentKeyPeriod@index 来跟踪密钥时段。
- 为了支持 MSS PlayReady，请在`DRMSystem`标签下SPEKE使用自定义参数`SPEKE:ProtectionHeader`。
- 对于HLS打包，如果响应中存在，则它必须包含要添加到HLS播放列表`EXT-X-KEY`标签URI参数中的完整数据，无需进一步的信号传输。`URIExtXKey`

- 对于HLS播放列表，在DRMSystem标签下方，SPEKE提供了可选的自定义参数speke:KeyFormatVersions，对于EXT-X-KEY标签speke:KeyFormat和参数的值，则KEYFORMAT提供了可选的自定义KEYFORMATVERSIONS参数。

  除非操作员明确指定，否则HLS初始化向量 (IV) 始终遵循分段编号。
- 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。
- SPEKE目前不支持每个内容有多个曲目或按键。

  SPEKE兼容的加密器充当客户端，并将POST操作发送到密钥提供程序端点。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。

SPEKEAPIv1-标准有效载荷组件

在任何SPEKE请求中，加密器都可以请求一个或多个DRM系统的响应。加密器指定请求负载<cpix:DRMSystemList>中的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。

以下示例显示了具有单一DRM系统规格的DRM系统列表：

```
<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	在 I DASH F 组织中注册的DRM系统类型的唯一标识符。有关列表，请参阅 DASH-IF 系统IDs。

标识符	描述
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。
<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>	请求特定于保护系统的标头 (PSSH)。作为 Common Encrypti systemID on (CENC) 的一部分kid，此类标头包含对DRM供应商的、和自定义数据的引用。密钥响应类型必须是此响应或 UriExtXKey 响应。

_标准密钥和 _ 的请求示例 PSSH

以下示例显示了加密器向DRM密钥提供者发出的部分示例请求，并突出显示了主要组件。第一个请求是标准密钥，而第二个请求是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 _ 的响应示例 PSSH

以下示例显示了DRM密钥提供者对加密器的相应响应：

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

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

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

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

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

SPEKEAPIv1-实时工作流程方法调用示例

请求语法示例

以下URL是一个示例，并不表示固定格式：

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

请求正文

一个CPIX元素。

请求标头

名称	Type	发生次数	描述
AWS Authorization	String	1..1	参见 AWSSigv4

名称	Type	发生次数	描述
X-Amz-Security-Token	String	1..1	参见 AWSSigv4
X-Amz-Date	String	1..1	参见 AWSSigv4
Content-Type	String	1..1	application/xml

响应标头

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

请求响应

HTTP CODE	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效载荷响应
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器到密DRM钥提供者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

以下示例显示了来自DRM密钥提供者的典型响应负载：

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

SPEKEAPIv1-VOD 工作流程方法调用示例

请求语法示例

以下URL是一个示例，并不表示固定格式。

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

请求正文

一个CPIX元素。

响应标头

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

请求响应

HTTP CODE	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效载荷响应
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。

VOD带有清除密钥的请求负载示例

以下示例显示了从加密器到密DRM钥提供者的基本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>
```

VOD带有清空密钥的响应负载示例

以下示例显示了来自DRM密钥提供者的基本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>
```

SPEKEAPIv1-内容密钥加密

您可以选择在SPEKE实现中添加内容密钥加密。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 Cloud 中运行的加密器使用内容密钥加密，客户需要将证书导入 Certificate Manager，然后使用生成的证书ARNs进行加密活动。AWS加密器使用证书ARNs和ACM服务向密钥提供者提供加密的DRM内容密钥。

限制

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

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

这些限制也列在 DASH-IF 规范的自定义和约束中。

实现内容密钥加密

要提供内容密钥加密，请在密DRM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>
```

SPEKEAPIv1-Heartbeat

请求语法示例

以下URL是一个示例，并不表示固定格式：

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

请求响应

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

SPEKEAPIv1-覆盖密钥标识符

每次轮换密钥时，加密器都会创建一个新的密钥标识符 (KID)。它会在请求中将传递KID给DRM密钥提供者。几乎总是密钥提供者使用相同的值进行响应KID，但它可以在响应KID中为提供不同的值。

以下是带有的示例请求 KID11111111-1111-1111-1111-111111111111：

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

以下响应会覆盖 t KID o22222222-2222-2222-2222-222222222222：

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

```
      <cpix:ContentKeyList>
       <cpix:ContentKey explicitIV="ASgwx9pQ2/2lnDzJsUxWcQ=="
 kid="22222222-2222-2222-2222-222222222222">
        <cpix:Data>
         <pskc:Secret>
          <pskc:PlainValue>p3dWaHARtL97MpT7TE916w==</pskc:PlainValue>
         </pskc:Secret>
        </cpix:Data>
       </cpix:ContentKey>
      </cpix:ContentKeyList>
      <cpix:DRMSystemList>
       <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
        <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOY
cpix:PSSH>
       </cpix:DRMSystem>
      </cpix:DRMSystemList>
      <cpix:ContentKeyPeriodList>
       <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
      </cpix:ContentKeyPeriodList>
      <cpix:ContentKeyUsageRuleList>
       <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222">
        <cpix:KeyPeriodFilter
 periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
       </cpix:ContentKeyUsageRule>
      </cpix:ContentKeyUsageRuleList>
     </cpix:CPIX>
```

SPEKEAPIv2

这是 Secure Packager 和 Encoder 密钥交换 (SPEKE) v2 的。REST API使用本规范为使用加密的客户提供DRM版权保护。为了SPEKE符合要求，您的DRM密钥提供程序必须公开本规范中RESTAPI描述的。加密器会API调用您的密钥提供商。

> **Note**
>
> 本规范中的代码示例仅用于说明目的。你无法运行这些示例，因为它们不是完整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重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HLSDASH、和。MSS

从其版本 2.0 开始SPEKE，与特定CPIX版本保持一致：

SPEKE一方面，这是通过使用X-Speke-VersionHTTP标题来强制执行的，CPIX另一方面是通过使用CPIX@version属性来强制执行的。请求中缺少这些元素是 SPEKE v1 传统工作流程的典型特征。在 SPEKE v2 工作流程中，只有当密钥提供程序同时支持两个版本参数时，它才需要处理CPIX文档。

有关交换格式的详细信息，请参阅DASH行业论坛 CPIX2.3 规范。

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

- 不推荐使用SPEKEXML命名空间中的所有标签，取而代之的是命名空间中的CPIXXML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
- 新的必填CPIX属性：CPIX@version，ContentKey@commonEncryptionScheme
- 新的可选CPIX元素：DRMSystem.ContentProtectionData
- 支持多个内容密钥
- 和之间的跨版本控制机制 SPEKE CPIX
- HTTP标题演变：新X-Speke-Version标题，标Speke-User-Agent题重命名为 X-Speke-User-Agent
- 心跳API已被弃用

由SPEKE于 v1.0 规范保持不变，因此无需更改现有实现即可继续支持 SPEKE v1.0 工作流程。

主题

- SPEKEAPIv2--IF 规范的自定义和约束 DASH
- SPEKEAPIv2-标准有效载荷组件
- SPEKEAPIv2-加密合约

- SPEKEAPIv2-实时工作流程方法调用示例
- SPEKEAPIv2-VOD 工作流程方法调用示例
- SPEKEAPIv2-内容密钥加密
- SPEKEAPIv2-覆盖密钥标识符

SPEKEAPIv2--IF 规范的自定义和约束 DASH

DASH行业论坛 CPIX2.3 规范支持多种用例和拓扑。SPEKEAPIv2.0 规范定义了CPIX配置文件和 fo API r。CPIX为了实现这两个目标，它遵守CPIX规范，并具有以下自定义和限制：

CPIX个人资料

- 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RSA基于 2048 的证书。
- SPEKE仅利用部分CPIX功能：
  - SPEKE 会忽略 `UpdateHistoryItemList` 功能。如果响应中存在该列表，则将其SPEKE忽略。
  - SPEKE省略了根/叶键功能。如果响应中存在该`ContentKey@dependsOnKey`属性，则将其SPEKE忽略。
  - SPEKE省略`BitrateFilter`元素和`VideoFilter@wcg`属性。如果CPIX有效载荷中存在这些元素或属性，则将其SPEKE忽略。
- 只有标准负载组件页面或加密合同页面上引用为 “支持” 的元素或属性才能用于与 SPEKE v2 交换的CPIX文档中。
- 当包含在加密器的CPIX请求中时，所有元素和属性都应在密钥提供者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。
- 要HLS发送信号，必须使用多个`DRMSystem.HLSSignalingData`元素：一个元素的`DRMSystem.HLSSignalingData@playlist`属性值为 “媒体”，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，密钥提供者应返回一个错误，描述为 “Missing CPIX @contentId”。 CPIX@contentId值不能被密钥提供者覆盖。

  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，密钥提供者应返回一个错误，描述为 “Miss CPIX ing @version”。当收到版本不支持的请求时，密钥提供程序返回的错误描述应为 “不支持 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个错误，描述为 “缺少 ContentKey @ f commonEncryptionScheme or KIDid”。

  一个唯一的CPIX文档不能混合不同ContentKey@commonEncryptionScheme属性的多个值。收到此类组合时，密钥提供者应返回一条错误信息，描述为 “不合规 ContentKey @ commonEncryptionScheme 组合”。

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

  ContentKey@commonEncryptionScheme 值不能被密钥提供程序覆盖。
- 当在CPIX响应正文中接收不同值DRMSystem@PSSH和DRMSystem.ContentProtectionData内部XML<pssh>元素时，加密器应停止并抛出错误。

API for CPIX

- 密钥提供者应包含X-Speke-User-AgentHTTP响应标头的值。
- SPEKE兼容的加密器充当客户端，并将POST操作发送到密钥提供程序端点。
- 加密器应包含X-Speke-VersionHTTP请求标头的值，请求中使用的SPEKE版本应表述为 MajorVersion。 MinorVersion，比如 SPEKE v2.0 的 “2.0”。如果密钥提供程序不支持加密器在当前请求中使用的SPEKE版本，则密钥提供程序将返回错误信息，并说明为 “不支持的SPEKE版本”，并且不要尝试尽力处理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，加密器应抛出错误，并且不会使用 SPEKE v1.0 版本重试请求。

  如果密钥提供程序没有返回错误但未能返回包含必填信息的CPIX文档，则加密器应停止并抛出错误。

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，切勿为 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	不见了 CPIX @version
CPIX不支持 @version	不支持 @version CPIX
ContentKey@ commonEncryptionScheme 未定义	缺少 ContentKey @ commonEncryptionScheme KIDid（其中id等于 ContentKey @kid 值）
在单个CPIX文档中使用多个 ContentKey @ commonEncryptionScheme 值	不合规的 ContentKey @ commonEncryptionScheme 组合
ContentKey@ commonEncryptionScheme 与DRM技术不兼容	ContentKey@ commonEncryptionScheme 不兼容 DRMSystemid（其中id等于 DRMSystem @ systemId 值）
X-Speke-Version 标头值不是支持的版本 SPEKE	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
加密合同与DRM安全级别限制相矛盾	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

SPEKEAPIv2-标准有效载荷组件

根据为给定内容定义的加密合约，通过单个SPEKE请求，加密器可以请求多个内容密钥，以及针对多种包装格式的必需的 manfest 信号。

为了涵盖所有这些方面，标准CPIX文档由三个必填列表部分和一个用于实时内容密钥轮换的可选列表部分组成。

<cpix: ContentKeyList > 分区和顶层<cpix : >元素 CPIX

这是一个必填部分，与VOD直播和流媒体相关，定义了加密器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，该ContentKey@commonEncryptionScheme属性的可能值在《ISO基本媒体文件格式文件中的通用加密》规范（ISO/IEC23001-7:2016）中定义：

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

以下示例显示了具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。

支持的元素 SPEKE	强制属性	可选属性	强制子元素	可选子元素
<cpix : >CPIX	contentId，版本，xmlns : cpix，xmlns: pskc	name、xmlns:enc	一个 <cpix: ContentKeyList >，一个<cpix : >，一个 <cpix: DRMSystem List > 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 EncryptedValue	价值 MAC	-	<enc: EncryptionMethod >，<enc : >CipherData

<cpix : >部分 DRMSystemList

这是一个必修部分，与VOD直播和流媒体有关，它定义了需要与内容密钥一起使用的不同DRM系统。

以下示例显示了具有单一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>
```

有关完整列表 DRMsystemIDs，请参阅 DASH-IF 标识符存储库的 “内容保护” 部分。

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

DRMSystem@PSSH如果 ISO-BMFF 封装应用于媒体段，则为必填项。
DRMSystem.ContentProtectionData加密器仅将内部XML<pssh>元素用于清单信令目的。

如果DRMSystem@PSSH存在且DRMSystem.ContentProtectionData包含内部XML<pssh>元素，则两个值应相同。

如果要在HLS清单中携带DRMSystem信号，则CPIX请求<cpix:HLSSignalingData playlist="media">和响应中必须同时包含 a 和 a <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>
```

支持的元素 SPEKE	强制属性	可选属性	强制子元素	可选子元素
<cpix : >ContentK eyPeriodList	-	id	至少有一个 <cpix : >ContentK eyPeriod	-
<cpix : >ContentK eyPeriod	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

这是一个必修部分，与VOD直播和流媒体有关，定义了不同的内容密钥将如何保护直播内和加密时期的曲目。

<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>
```

支持的元素 SPEKE	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, hdrminFps, 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。

SPEKEAPIv2-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首曲目是可能的，但需要在加密器发送给密钥提供者的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

加密合同位于CPIX文档的<cpix:ContentKeyUsageRuleList>部分中。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定义了多个过滤元素和属性，但仅SPEKE支持其中的一部分。下表对这些不同情况进行了汇总：

CPIX过滤器类型	总体SPEKE支持	支持的筛选器属性SPEKE	不支持的筛选器属性SPEKE
<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（必填属性）	
<cpix : >BitrateFilter	否	不适用	不适用
<cpix : >LabelFilter	否	不适用	不适用

根据CPIX规范 VideoFilter，[minPixels，maxPixels] 是两个维度的全包范围，而 (minFps,maxFps] 仅包含该 maxFps 维度。因为 AudioFilterminChannels，[，maxChannels] 是两个维度的包含范围。

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）	加密器应查看其配置（CPIX有效载荷外部），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。

在这种情况下	加密程序器应该...	密钥提供程序应该...
加密合同在单个SPEKE请求/响应周期内发生变化	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。	首先，为了防止这种情况发生，密钥提供者不得修改SPEKE请求CPIX有效载荷中收到的加密合约。
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	加密器应引发异常，停止处理并且不向密钥提供者发送SPEKE请求，因为这很可能会导致错误的内容保护或使某些曲目不受保护。	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。
格式良好的加密合同，但违反了DRM安全级别的限制：例如，要求使用单个内容密钥来保护音轨和UHD视频轨道	如果加密器知道DRM安全级别限制，则应引发异常，停止处理，不要将SPEKE请求发送给密钥提供者，因为这很可能会导致错误的内容保护。	密钥提供者应引发异常并返回“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 AudioFilter 内容 VideoFilter 或元素的CPIX文档。	密钥提供者应引发异常并返回“缺少CPIX加密合同” 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：不同的视频轨道有多个内容键（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：不同的视频轨道有多个内容键（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（SDHD1/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>
```

SPEKEAPIv2-实时工作流程方法调用示例

请求语法示例

以下URL是一个示例，并不表示固定格式：

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

请求正文

一份CPIX文档。

请求标头

名称	Type	发生次数	描述
`AWS Authorization`	String	1..1	参见 AWSSigv4
`X-Amz-Security-Token`	String	1..1	参见 AWSSigv4
`X-Amz-Date`	String	1..1	参见 AWSSigv4
`Content-Type`	String	1..1	application/xml

名称	Type	发生次数	描述
X-Speke-Version	String	1..1	SPEKEAPI与请求一起使用的版本，表述为 MajorVersion。MinorVersion，比如 SPEKE v2.0 的 “2.0”

响应标头

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

请求响应

HTTP CODE	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效载荷响应
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器到DRM密钥提供者的典型实时请求负载，所有视频轨道都有一个内容密钥，所有音轨都有一个内容密钥：

```
<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密钥提供者的典型响应负载（为了便于阅读，返回值已缩短为 [...]）：

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
  <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
   <cpix:Data>
    <pskc:Secret>
     <pskc:PlainValue>h3toSFIlyAYpfXVQ795m6x==</pskc:PlainValue>
    </pskc:Secret>
   </cpix:Data>
  </cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- FairPlay -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
   <cpix:HLSSignalingData playlist="media">trBAnbMcj[...]u44</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
  </cpix:DRMSystem>
  <!-- Widevine -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[...]nNB</cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
   <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
   <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
  </cpix:DRMSystem>
  <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
```

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

SPEKEAPIv2-VOD 工作流程方法调用示例

请求语法示例

以下URL是一个示例，并不表示固定格式。

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

请求正文

一份CPIX文档。

请求标头

名称	Type	发生次数	描述
AWS Authorization	String	1..1	参见 AWSSigv4
X-Amz-Security-Token	String	1..1	参见 AWSSigv4
X-Amz-Date	String	1..1	参见 AWSSigv4
Content-Type	String	1..1	application/xml
X-Speke-Version	String	1..1	SPEKEAPI与请求一起使用的版本，表述为 MajorVersion。MinorVersion，比如 SPEKE v2.0 的 “2.0”

响应标头

名称	Type	发生次数	描述
X-Speke-User-Agent	String	1..1	用于标识密钥提供程序的字符串

名称	Type	发生次数	描述
Content-Type	String	1..1	application/xml
X-Speke-Version	String	1..1	SPEKEAPI与请求一起使用的版本，表述为 MajorVersion。MinorVersion，比如 SPEKE v2.0 的 “2.0”

请求响应

HTTP CODE	负载名称	发生次数	描述
200 (Success)	CPIX	1..1	DASH-CPIX 有效载荷响应
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。

VOD带有清除密钥的请求负载示例

以下示例显示了从加密器到DRM密钥提供者的典型VOD请求负载，所有视频轨道都有一个内容密钥，所有音轨都有一个内容密钥：

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
```

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

```
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
   <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
 intendedTrackType="VIDEO">
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
 intendedTrackType="AUDIO">
   <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

VOD带有清空密钥的响应负载示例

以下示例显示了来自DRM密钥提供者的典型响应负载（为了便于阅读，返回值已缩短为 [...]）：

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

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

```
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
   </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyUsageRuleList>
   <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="VIDEO">
    <cpix:VideoFilter />
   </cpix:ContentKeyUsageRule>
   <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
  intendedTrackType="AUDIO">
    <cpix:AudioFilter />
   </cpix:ContentKeyUsageRule>
  </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKEAPIv2-内容密钥加密

您可以选择在SPEKE实现中添加内容密钥加密。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 Cloud 中运行的加密器使用内容密钥加密，客户需要将证书导入 Certificate Manager，然后使用生成的证书ARNs进行加密活动。AWS加密器使用证书ARNs和ACM服务向密钥提供者提供加密的DRM内容密钥。

限制

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

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

这些限制也列在 DASH-IF 规范的自定义和约束中。

实现内容密钥加密

要提供内容密钥加密，请在密DRM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>
```

SPEKEAPIv2-覆盖密钥标识符

每次轮换密钥时，加密器都会创建一个新的密钥标识符 (KID)。它会在请求中将传递KID给DRM密钥提供者。几乎总是密钥提供者使用相同的值进行响应KID，但它可以在响应KID中为提供不同的值。

以下是带有的示例请求 KID11111111-1111-1111-1111-111111111111：

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
 xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
 <cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="
 kid="11111111-1111-1111-1111-111111111111" commonEncryptionScheme="cbcs"></
cpix:ContentKey>
 </cpix:ContentKeyList>
 <cpix:DRMSystemList>
  <!-- Widevine -->
```

```
  <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
 systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
   <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
   <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
   <cpix:ContentProtectionData></cpix:ContentProtectionData>
   <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>
 </cpix:DRMSystemList>
 <cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
 index="1" />
 </cpix:ContentKeyPeriodList>
 <cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111"
 intendedTrackType="VIDEO">
   <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
   <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
 </cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

以下响应会覆盖 t KID o22222222-2222-2222-2222-222222222222：

```
<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>
```

该SPEKEAPI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. 有效的技术措施是指在没有适当授权的情况下，根据履行1996年12月20日通过的《WIPO版权条约》第11条规定的义务的法律和/或类似的国际协议，不得规避的措施。

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. 不会根据本公共许可证授予道德权利 (如诚信权)，也不授予公开权、隐私权和/或其他类似的人格权利；不过，在可能的范围内，许可人在一定程度上放弃和/或同意不主张拥有的任何这些权利，以使您能够行使许可权利。
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获得许可的，并包括本公共许可证的文本或指向本公共许可证的超链接。URI

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，通过提供包含所需信息的资源的URI或超链接来满足这些条件可能是合理的。
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演绎材料，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. 您必须附上您申请的适配器许可证的文本、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

下表描述了对SPEKE文档的更改。

SPEKE v1

更改	描述	日期
Support matrix：AWS合作伙伴服务和产品	在AWS合作伙伴服务和产品中添加了新的SPEKE支持部分，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了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
Support matrix—— AWS 元素直播	添加了 E AWS lemental Live 支援矩阵。	2018 年 9 月 27 日
标准负载组件	添加了定义JSON有效载荷中主要元素的部分。	2018 年 9 月 27 日
KID覆盖	添加了有关密钥提供者KID替换的部分。	2018 年 9 月 27 日
更正了指向 DASH-IF 网站的链接	更正了指向 I DASH F 网站的CPIX规范和系统IDs页面的链接。	2018 年 9 月 27 日
AWSElemental Live 的发行副本	更新了SPEKE文档，添加了AWS Elemental 产品。	2018 年 7 月 20 日

更改	描述	日期
CMAF	更新了服务的支持矩阵表，使其包含通用媒体应用程序格式 (CMAF)。	2018 年 6 月 27 日
初始版本	Secure Packager 和 Encoder Key Exchange (SPEKE) 版本 1 的初始版本，这是内容加密器和DRM密钥提供者之间通信的规范。DRM密钥提供程序公开安全打包程序和编码器密钥交换API以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AWS服务和产品支持SPEKE部分的更新	将 Webstream 添加到DRM平台提供商列表的 SPEKE v2 列中，并添加 MediaConvert 到“AWS服务和产品SPEKE支持”表的 SPEKE v2 列中。	2024 年 10 月 10 日
DRM平台提供商部分的更新	在DRM平台提供商列表的 SPEKE v2 列中添加了新的合格合作伙伴。	2023 年 8 月 9 日
Live 和VOD工作流方法调用示例部分的更新	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
DRM平台提供商和加密合同部分的更新	在DRM平台提供商列表的 SPEKE v2 列中添加了新的合格合作伙伴。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	Secure Packager 和 Encoder Key Exchange (SPEKE) 版本 2.0 的初始版本，这是内容加密器和DRM密钥提供者之间通信的规范。DRM密钥提供程序公开安全打包程序和编码器密钥交换API以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。