Secure Packager and Encoder Key Exchange (SPEKE)

Open API Specification for Encoders, Transcoders, Packagers, and DRM Platforms

aws insights

aws

Agenda

- Key Terms
- SPEKE (Secure Packager Encoder Key Exchange)
- Advantages
- SPEKE Architecture

What is the SPEKE API?

The **S**ecure **P**ackager and **E**ncoder **K**ey **E**xchange (SPEKE) is an open API specification which defines the standard for communication between encryptors and digital rights management (DRM) platforms.

Key Terms

Encryptor
- Encoders, transcoders, packagers

CPIX
- Content Protection Information Exchange format (DASH-IF)

SystemID or **schemeId**
- Unique ID for the underlying DRM vendor:
  - Microsoft PlayReady: `9a04f079-9840-4286-ab92-e65be0885f95`
  - Google Widevine: `edef8ba9-79d6-4ace-a3c8-27dcd51d21ed`
- Registered at: https://dashif.org/identifiers/protection/

Key ID (KID)
- Identifier that points to the underlying Key similar to a hash table

PSSH
- Protection System Specific Header, as part of CENC (Common Encryption)
- Contains a reference to the KeyID, SystemID and custom data for that DRM vendor Stored as an MP4 box in fMP4
- Stored as base64 encoding for MP4 box in DASH MPD

Why do we need to use DRMs?

Protect and control access to content

- Monetize content by maintaining control and fulfillment

Market coverage

- Content producers protect Premium video content
- Sporting events example: FIFA WorldCup 2018

Playback Complexity

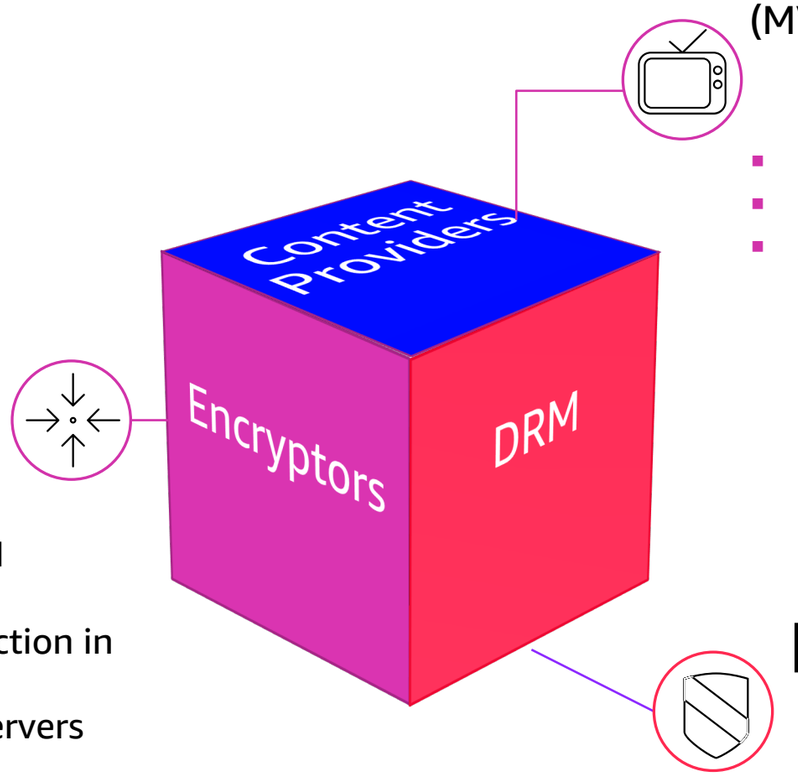
- Consumers watch content on various devices which all have specific Container/DRM requirements
- The DASH container offers Multi-DRM protected using Widevine and PlayReady
- Apple HLS is protected using Apple Fairplay
- Playback on Web Browsers, Multiscreen devices and Set-top boxes

SPEKE – Democratization of the video workflow

Content Providers

(MVPDS and Content distributors)

- Lowers barrier of DRM solution provider adoption
- Opportunity cost savings with quicker integration
- Ability to expand audience/device coverage



Encryptors

(Encoders, Transcoders and Packagers)

- Robust and lighter application
- Saves time, effort and cost of custom DRM API integration (4 weeks per custom integration)
- Savings in testing time and effort (~17% reduction in testing effort)
- Ability to test DRM workflow with reference servers

DRM Solution Providers

- Lowers barrier to adoption
- Custom integration cost and time savings
- Ability to establish proven workflows

aws insights

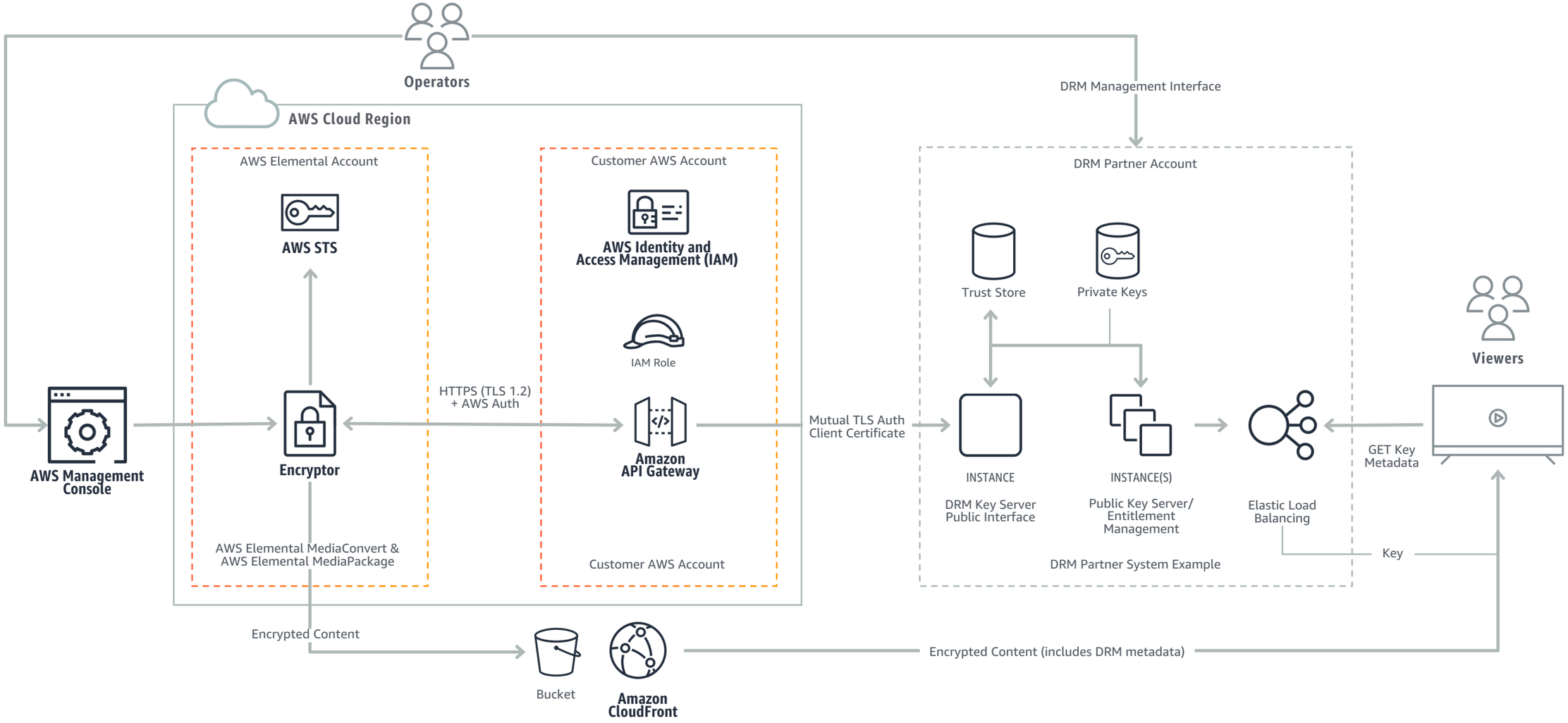
aws

The SPEKE Ecosystem

Several DRM Solution providers have implemented SPEKE

SPEKE also enables customers to develop their own key management solution

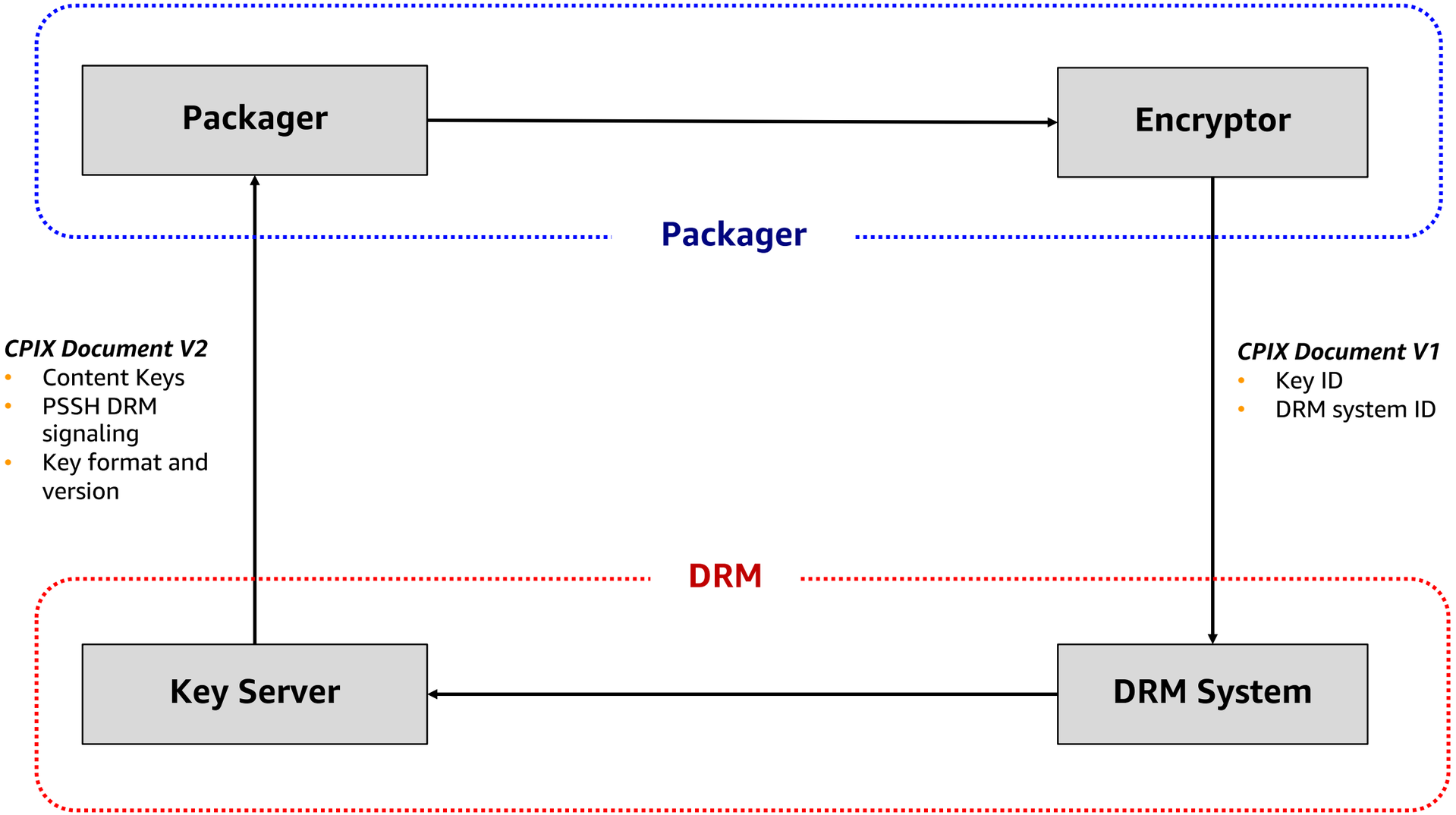
SPEKE System Diagram



aws insights

aws

SPEKE – CPIX Based Encryptor Consumer Model



aws insights

aws

SPEKE Request Sample – XML POST Over HTTP

```
<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>
<!-- 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:CPIX>
```

GET Key

KeyID

SystemID 1

KeyID

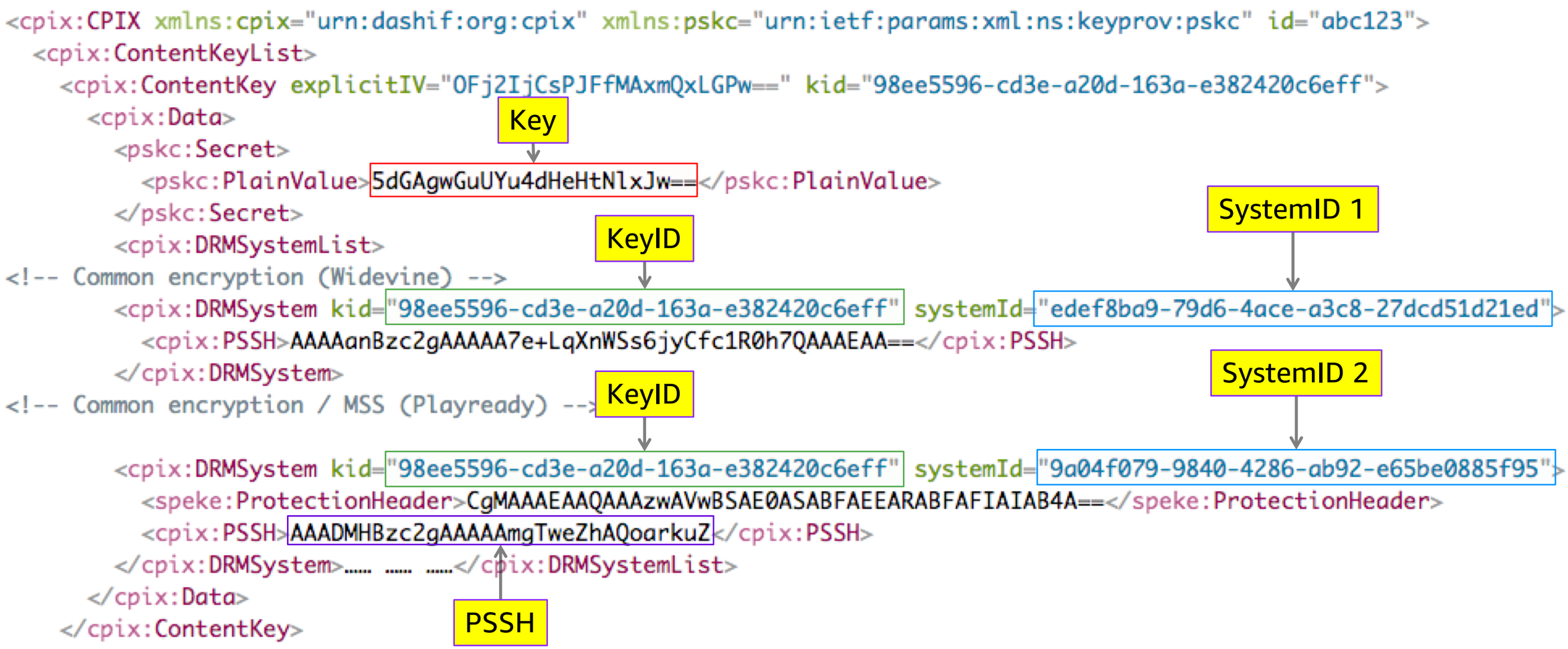
SystemID 2

GET PSSH

aws insights

aws

SPEKE Response Sample – XML Over HTTP




```
<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix" xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc" 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:DRMSystemList>
<!-- Common encryption (Widevine) -->
        <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
          <cpix:PSSH>AAAAanBzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAAEAA==</cpix:PSSH>
        </cpix:DRMSystem>
<!-- Common encryption / MSS (Playready) -->
        <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="9a04f079-9840-4286-ab92-e65be0885f95">
          <speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABBFAEEARABFAFIAIAB4A==</speke:ProtectionHeader>
          <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZ</cpix:PSSH>
        </cpix:DRMSystem>..... ..... .....</cpix:DRMSystemList>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
</cpix:CPIX>
```

aws insights

aws

How Do I Get Started with SPEKE?

- SPEKE API Documentation: https://docs.aws.amazon.com/speke/latest/documentation/what-is-speke.html
- SPEKE reference server: https://github.com/awslabs/speke-reference-server

SPEKE Reference Server

- Open source reference key server in GitHub AWS Labs project area
- Foundational example of a custom SPEKE key server
- Available today for use and customization
- Provides pre-built CloudFormation templates and code for a turnkey installation
- Integrates API Gateway, Lambda, S3, CloudFront, Secrets Manager for key generation
  - Uses secret IV per stream (content ID)
  - Uses key derivation to produce encryption/decryption keys
- Supports HLS, HLS-Sample, and DASH
- Participate at https://github.com/awslabs/speke-reference-server
- Fork the project and build your own key server
- Submit issues, questions, pull requests with improvements

Additional Resources:

- DASH-IF Implementation Guidelines: Content Protection Information Exchange Format (CPIX): http://dashif.org/wp-content/uploads/2016/11/DASH-IF-CPIX-v2-0.pdf
- Google Widevine: https://storage.googleapis.com/wvdocs/Widevine_DRM_Encryption_API.pdf
- Microsoft PlayReady: https://docs.microsoft.com/en-us/playready/
- Apple FairPlay Streaming: https://developer.apple.com/streaming/fps/

FAQ

- Can SPEKE be used for VOD and Live workflows?
- Is SPEKE extensible to new DRM systems?
- The encryptor creates the KID. Can the KID be overwritten?
- Can we integrate our own homegrown Key Management Server with SPEKE?
- How do you secure the communication channel for key exchange?

Thank you.

Ian McPherson

ianmcp@amazon.com