BUYDRM

CONTENT PROTECTION IN MPEG-DASH

JULY 2018, MILE HIGH VIDEO, DENVER

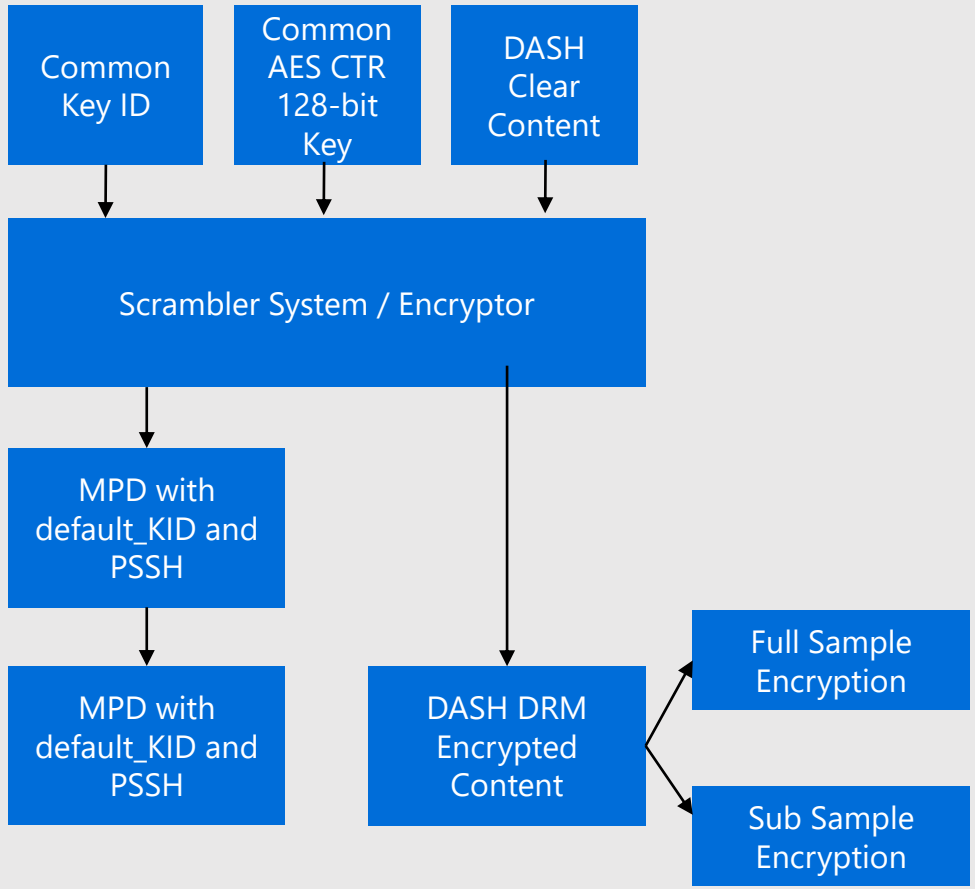
CONTENT PROTECTION AND SECURITY

- DASH-IF IOP provides a framework for multiple DRMs to protect DASH content by adding instructions:
  - Protection System Specific Information
  - Proprietary information in predetermined locations in MPDs or
  - DASH Content that is encrypted with CENC as defined in ISO/IEC 23001-7
- Common Encryption Schema (cenc)
  - Specifies encryption parameters
  - Key mapping methods (common KID)
  - The DRM scheme for each pssh is identified by a DRM specific SystemID
- The Base Technologies Summary
- ISO BMFF Support for Common Encryption and DRM
- MPD Support for Encryption and DRM Signaling
- Additional Content Protection Constraints
- Transport security in HTTP-based delivery

COMMON ENCRYPTION IN MPEG-DASH

- The normative standard that defines common encryption with ISO BMFF is ISO/IEC 23001-7 includes:
  - Common Encryption (CENC) of NAL structure video and other media data with AES 128 CTR mode
  - CBC Mode is also supported within CENC but not in DASH IF IOPs
- Support for decryption of a single Representation by multiple DRM Systems
- Key Rotation
- XML Syntax for expressing a default KID attribute and pssh element in MPDs

COMMON ENCRYPTION IN MPEG-DASH



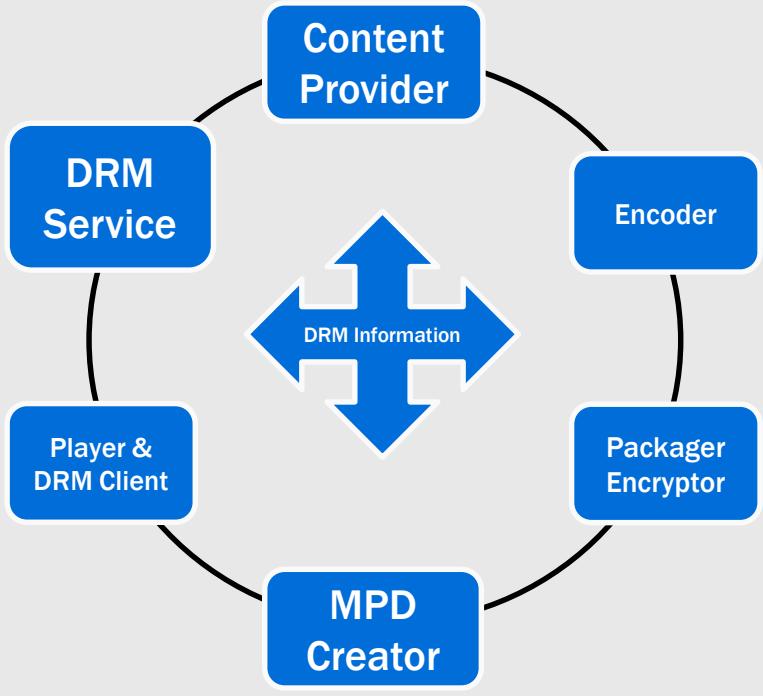
Simplified illustration of content encryption using common key

BASE TECHNOLOGY SUMMARY

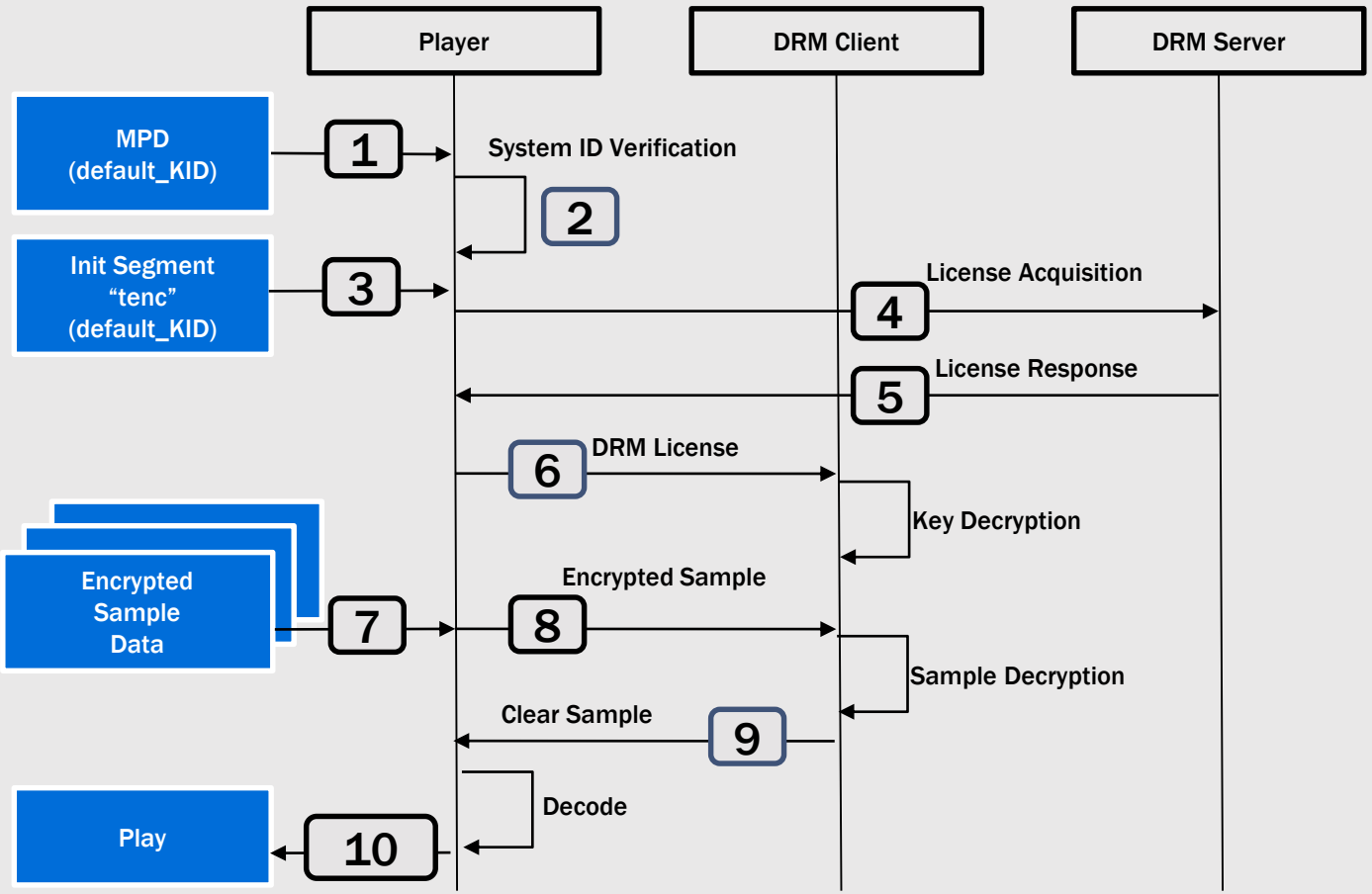
- Main DRM Components:
- ContentProtection Descriptors in the MPD
  - URI for signaling or
  - specific DRM being used
- Parameters that specify encryption parameters and default_KID (tenc)
- Parameters that may store initialization vectors and subsample encryption ranges (senc)
- License acquisition data or keys for each DRM in a format that is “Protection System Specific” (pssh)
- Key rotation is mainly used to allow changes in entitlement for continuous live content

WORKFLOW OVERVIEW

DRM Content Keys can be provided through ”Content Protection Information Exchange Format” v2.0



INFORMATION FLOW. DRM LICENSE RETRIEVAL



ENCRYPTION AND DRM SIGNALING

ContentProtection Descriptor for mp4protection Scheme

```
<ContentProtection schemeIdUri="urn:mpeg:dash:mp4protection:2011"
value="cenc" cenc:default_KID="34e5db32-8625-47cd-ba06-68fca0655a72"/>
```

Signals that content is encrypted with the scheme indicated in the **@value** attribute

ContentProtection Descriptor for UUID Scheme

```
<ContentProtection schemeIdUri="urn:uuid:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" value="DRMNAME version"/>
```

Protection System Specific Header Box cenc:pssh element in MPD

'pssh' Box data in MPD

A UUID may indicate the availability of a particular DRM scheme for license acquisition

```
<ContentProtection schemeIdUri="urn:uuid:d0ee2730-09b5-459f-8452-200e52b37567"
      value="2.0">

      <!– base64 encoded contents of 'pssh' box with this SystemID –>
      <acme ::pssh>
        YmFzZTY0IGVuY29kZWQgY29udGVudHMgb2YgkXB
        zc2iSIGJveCB3aXRoIHRoaXMgU3lzdGVtSUQ=
      </acme::pssh>
</ContentProtection>
```

The contents of the data array specified in the 'pssh' box is defined by each DRM system for use with their registered SystemID, and the same data array can be stored in the MPD within a ContentProtection Descriptor for UUID scheme

TRANSPORT AND SECURITY IN HTTP BASED DELIVERY

MPEG-DASH explicitly permits the use of https as a scheme and hence, HTTP over TLS as transport protocol

All media segments can be delivered over HTTPS by declaring <BaseURL>

```
<BaseURL>https://cdn1.example.com/</BaseURL>
<BaseURL>https://cdn2.example.com/</BaseURL>
```

Impacts of using HTTPs in DASH:

- CDN
  - It causes difficulties in caching encrypted DASH segment content
- Network
  - For underlying networks impossible to manage and optimize encrypted data traffics
- Efficiency
  - "double encryption" when streaming content is already encrypted using DRM. HTTPs add extra encryption overhead and therefore latency in streaming

KEYOS MULTI-DRM OTT PRODUCTS

DASH AND CPIX COMPATIBLE

KeyOS MultiPack

Standards-based Content Encryption Solution for On-Premise, In-Datacenter and In-The-Cloud deployments. Supports all three popular consumer DRMs and formats for VOD and Live. Integrated with KeyOS MultiKey Service and supported via NGINX Server.

KeyOS MultiKey

DRM as a Service (DaaS) Platform based on Multi-DRM concept. API- based for content encryption keys acquisition and content license key delivery. Supports all popular formats and DRMs, streaming / downloads and all popular playback platforms.

KeyOS MultiPlay

Device SDKs for Android and iOS platforms providing a feature-rich player, extensive multi-DRM / multi-format support, and an integrated download manager. Deployed inside customer-built Google Play and/or Apple iTunes premium application.

Facebook:
www.facebook.com/buydrm

Twitter:
www.twitter.com/buydrm

LinkedIn:
www.linkedin.com/company/buydrm

THANK YOU
ANDREW POPOV, CTO
ANDREW@KEYOS.COM

WWW.BUYDRM.COM