Advanced Web Technologies
Web & Media II

Stefan Pham | Open Distributed Systems | lecture winterterm 2015/16

Agenda

Datum		Inhalt
KW 43	27.10.2016	Introduction and framework
KW 44	3.11.2016	Web and Media I
KW 45	10.11.2016	Web and Media II
KW 46	17.11.2016	Web Technologies Basics
KW 47	24.11.2016	TV Apps
KW 48	1.12.2016	Multiscreen Technologies and Standards I
KW 49	8.12.2016	Multiscreen Technologies and Standards II
KW 50	15.12.2016	Data Mining & Recommender Systems
KW 51		Thema IX (oder Weihnachtsquiz)
KW 52		-
19.12.2016 - 02.01.2017		Weihnachtsferien
KW 01	5.1.2017	Web Of Things
KW 02	12.1.2017	WebSecurity and Privacy
KW 03	19.1.2017	Exkursion zum Fraunhofer FOKUS
		Treffpunkt um ### Uhr am Fraunhofer Institut FOKUS
KW 04	26.1.2017	Große Übung
KW 05 oder 06	9.2.2017	Schriftlicher Test (ca. 60 min)

Updates:

Per mail / in den VL Terminen

http://www.ods.tu-berlin.de/menue/lehre/wintersemester/vl_advanced_web_technologies/

Open Distributed Sytems
ODS

Project: Advanced Web Technologies

MEDIA STREAMING

Technische Universität Berlin

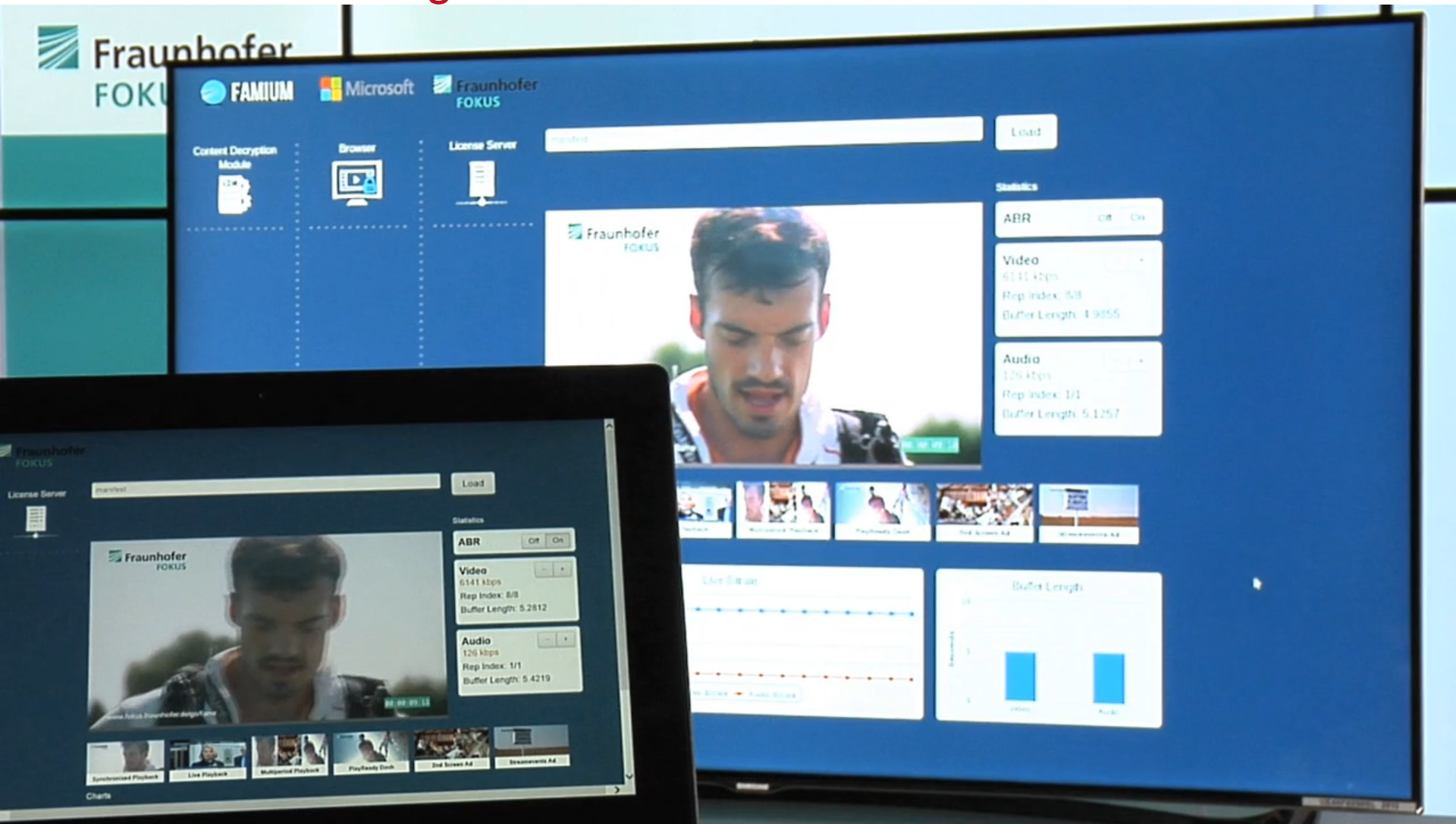
Topics:

- Accurate Bandwidth Limitation
- Server side re-encryption of MPEG-DASH based media streaming content
- Implementation of an MPEG-DASH segmenter using Node.js
- Development of real-time video and audio workflows using high performance processing software
- JavaScript-based Media Stream Manipulation
- Context-sensitive Adaptive Media Streaming
- Optimizing Media Streaming using Next Generation Web protocols
- Adaptive Streaming of 360° and panoramic videos

Open Distributed Sytems
ODS

Technische Universität Berlin

Media Streaming



ACCURATE BANDWIDTH LIMITATION

Student Project (1-3 participants), Bachelor thesis

- Use case: To measure the performance of different adaptive streaming algorithms, bandwidth fluctuations need to be emulated.
- Tasks:
  - Setup a HTTP proxy server that allows accurate shaping of the output bitrate.
  - Develop a small application to test and verify the accuracy of your setup.

- Related technologies: Linux Traffic Control and Token Bucket Filter

SERVER SIDE RE-ENCRYPTION OF MPEG-DASH BASED MEDIA STREAMING CONTENT

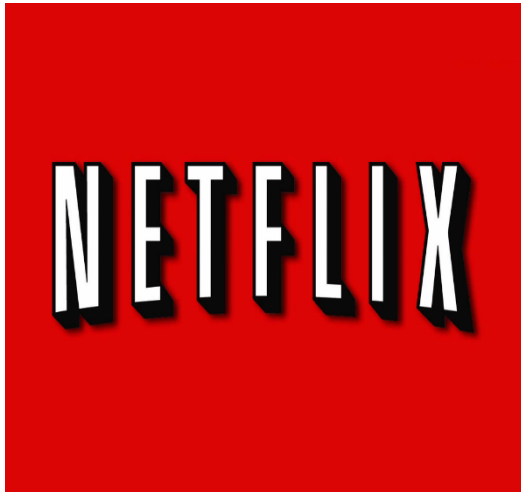
Student Project (1-3 participants), Bachelor thesis

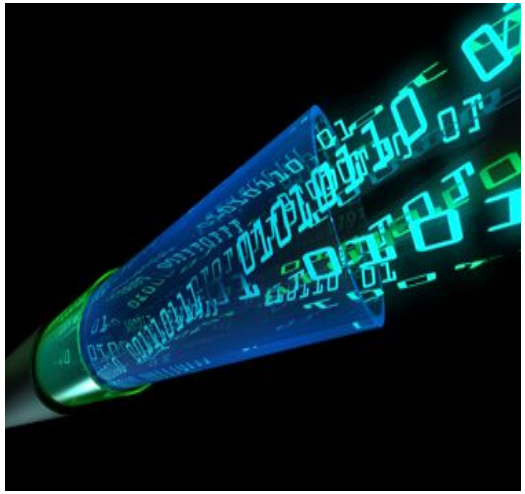
- Use case: Digital Rights Management (DRM) systems control the use of copyrighted content. Different combinations of operating systems and browsers require different DRM systems and therefore different encryption schemes.
- Tasks:
  - Understand the principles behind the encryption mechanisms used in DASH and HLS.
  - Analyze on the fly repackaging from encrypted DASH content into HLS.
  - If applicable implement a prototype for demonstration purposes.
- Related technologies: C/C++ or JavaScript/Node.js, MPEG-DASH, HLS

IMPLEMENTATION OF AN MPEG-DASH SEGMENTER USING NODE.JS

Student Project (1-3 participants), Bachelor thesis

- Use case: MPEG-DASH is a standard to enable adaptive media streaming in the browser using conventional HTTP servers. DASH conformant content is encoded in different qualities and segmented into small chunks.
- Tasks:
  - Understand the container structure of DASH based media files (ISOBMFF).
  - Extend a Node.js based DASH segmenter to support new box types.
  - Implement an MPD creator to support use cases like multi-period, ad-insertion.
- Related technologies: MPEG-DASH, JavaScript, Node.js





Fraunhofer FOKUS

DEVELOPMENT OF REAL-TIME VIDEO AND AUDIO WORKFLOWS USING HIGH PERFORMANCE PROCESSING SOFTWARE

Student Project (1-3 participants)

- Use case: High performance encoding and transcoding software has become an important part in the media distribution chain. In this context students will have the opportunity to take a deeper look into the latest high-end encoding software.
- Tasks:
  - Configuration of next generation encoding/packaging software.
  - Define your own encoding chains and test them in different players.
- Related technologies:Elemental Delta, Elemental Live, Thomson VS7000, Envivio Muse and Envivio Halo

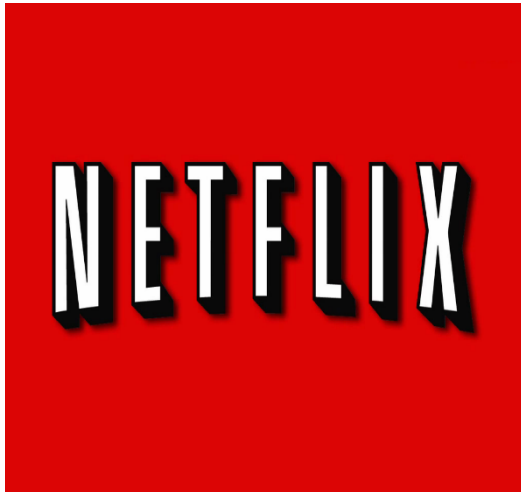
JAVASCRIPT-BASED MEDIA STREAM MANIPULATION

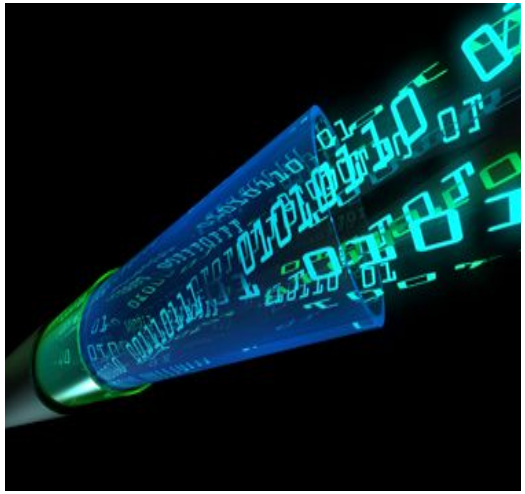
Student Project (1-3 participants), Bachelor- and Master Thesis

- Use case: Open source JavaScript-based frameworks such as isoboxer and mp4box.js enable extraction and manipulation of media streams.

- Tasks:
  - Research and develop use cases.
  - Analyze and extend frameworks for media stream manipulation.

- Related technologies: MPEG-DASH, JavaScript, Node.js





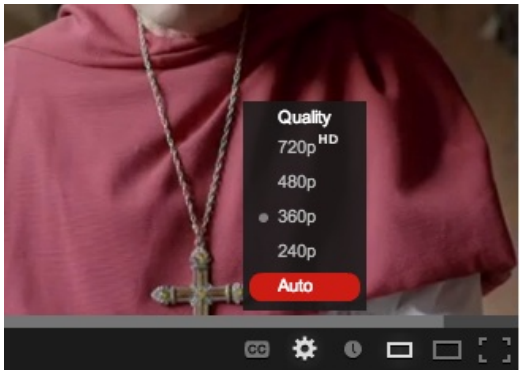
CONTEXT-SENSITIVE ADAPTIVE MEDIA STREAMING

Student Project (1-3 participants), Bachelor- and Master Thesis

- Use case: Adaptive media streaming solutions adjust the quality of video and audio content depending on the current available bandwidth on the client. The key component is the adaptivity algorithm of the client.

- Tasks:
  - Research & develop context-sensitive adaptive media streaming algorithms.
  - Integration with open source MPEG-DASH players (e.g. dash.js, Shaka).

- Related technologies: MPEG-DASH, JavaScript



OPTIMIZING MEDIA STREAMING USING NEXT GENERATION WEB PROTOCOLS

Student Project (1-3 participants), Bachelor- and Master Thesis

- Use case: Media streaming over HTTP 1.1 is based on a client-side pull mechanism. Next Generation Web protocols such as HTTP/2 or QUIC promise to reduce transmission latency by allowing server push mechanisms
- Tasks:
  - Research next generation Web protocols.
  - Investigate improvements with regard to media streaming latency.
- Related technologies: MPEG-DASH, SSE, HTTP/2, WebSockets, QUIC

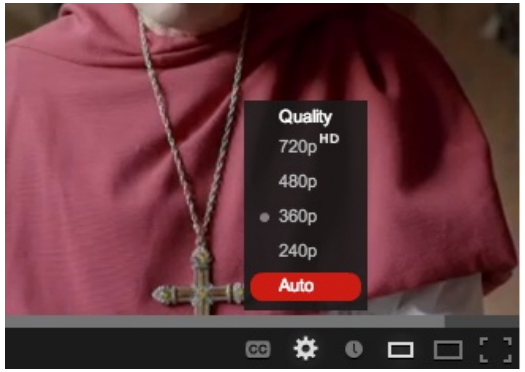
ADAPTIVE STREAMING OF 360° AND PANORAMIC VIDEOS

Student Project (1-3 participants), Bachelor- and Master Thesis

- Use case: Viewer can dynamically switch between different available regions in the video, for example a sports stadium.

- Task:
  - Research and develop use cases.
  - Extend adaptive streaming players (dash.js, Shaka player) to support streaming of 360° videos.

- Related technologies: MPEG-DASH, JavaScript



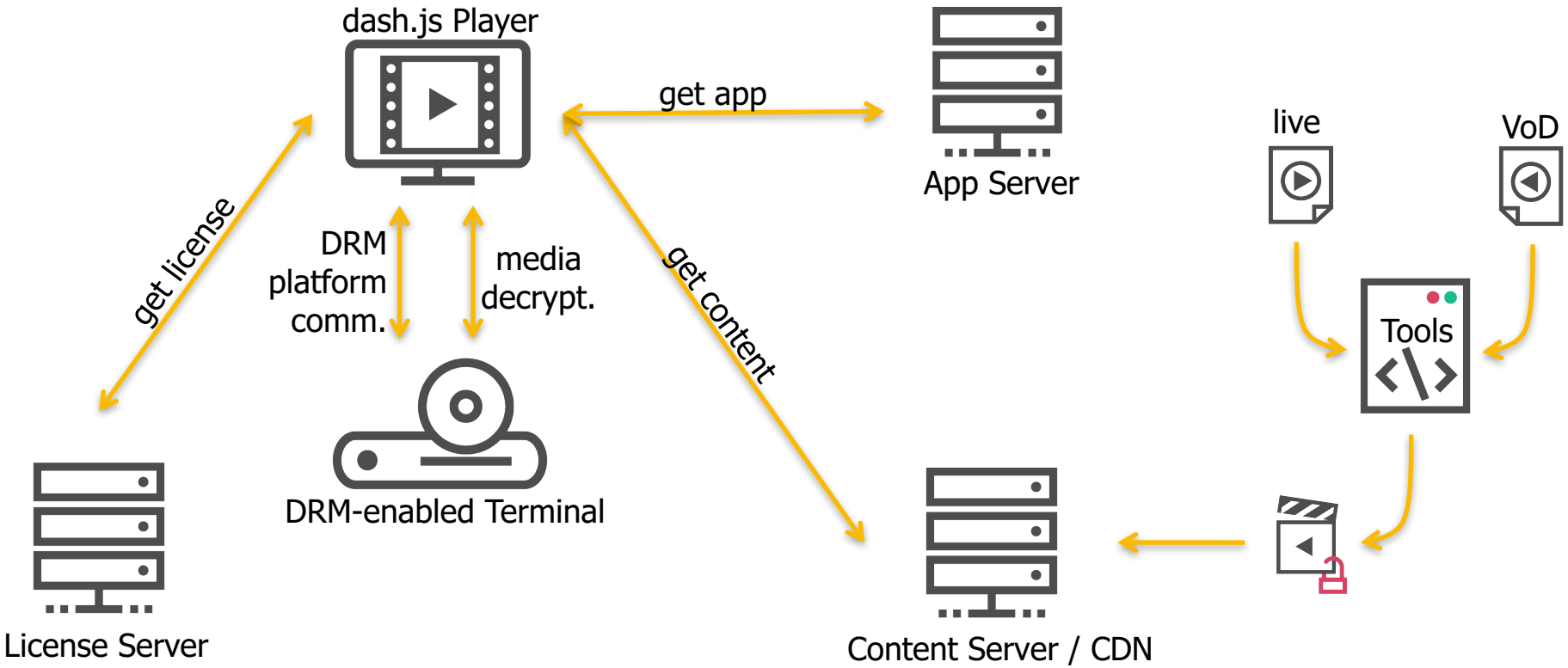
Agenda

- Recap Web & Media I
- Digital Rights Management (DRM)
- Common Encryption (CENC)
  - Demo: Stream Analysis
- Encrypted Media Extension (EME)
  - Demo: Multi-DRM Playback
- Reaching Streaming Devices
- Live Streaming

Web & Media II

Recap Web Media I

PLAYER ARCHITECTURE

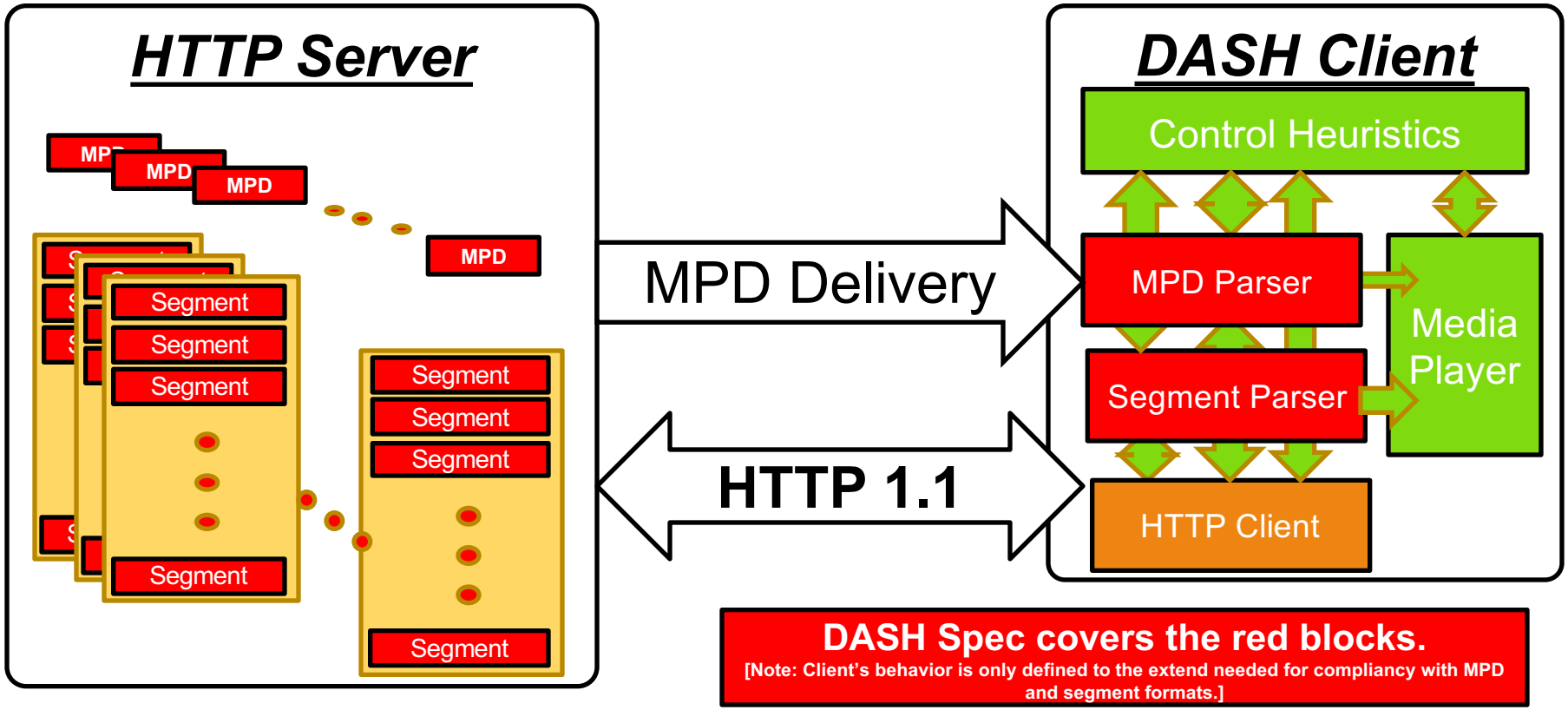


DELIVERING MEDIA: TECH TO UNDERSTAND

- **DASH** – MPEG **Dynamic Adaptive Streaming over HTTP** for live and on demand video
- **HLS** – Apple **HTTP Live Streaming** for live and on demand video
- **CENC** – MPEG **Common Encryption** for multi-DRM
- **MSE** – W3C **Media Source Extension** to trick-function HTML5 video-objects via JavaScript (control AV media streams)
- **EME** – W3C **Encrypted Media Extension** to play back DRM-protected media in standard browsers w/o the use of proprietary plug-ins
- **CDM** – **Content Decryption Module** - addition to the browser that provides functionality for one or more Key Systems

Fraunhofer FOKUS

MPEG-DASH - SCOPE

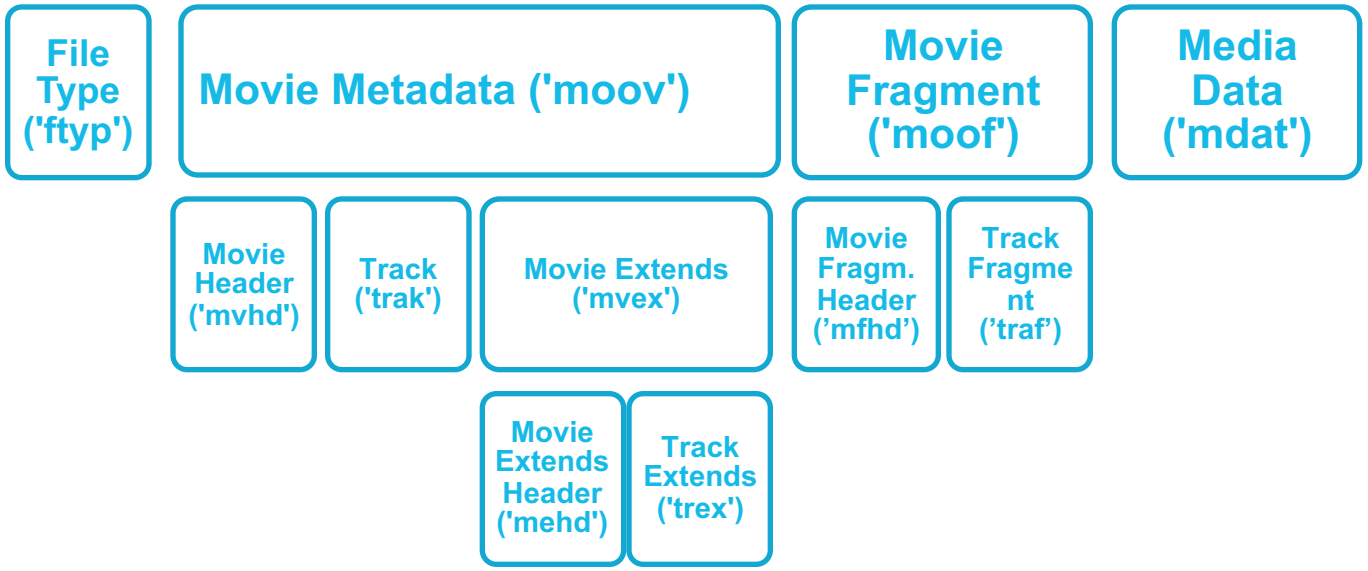


Fraunhofer FOKUS

MPEG-DASH FILE FORMAT

- ISO base media file format (ISOBMFF) or MPEG2-TS
- Codec-agnostic

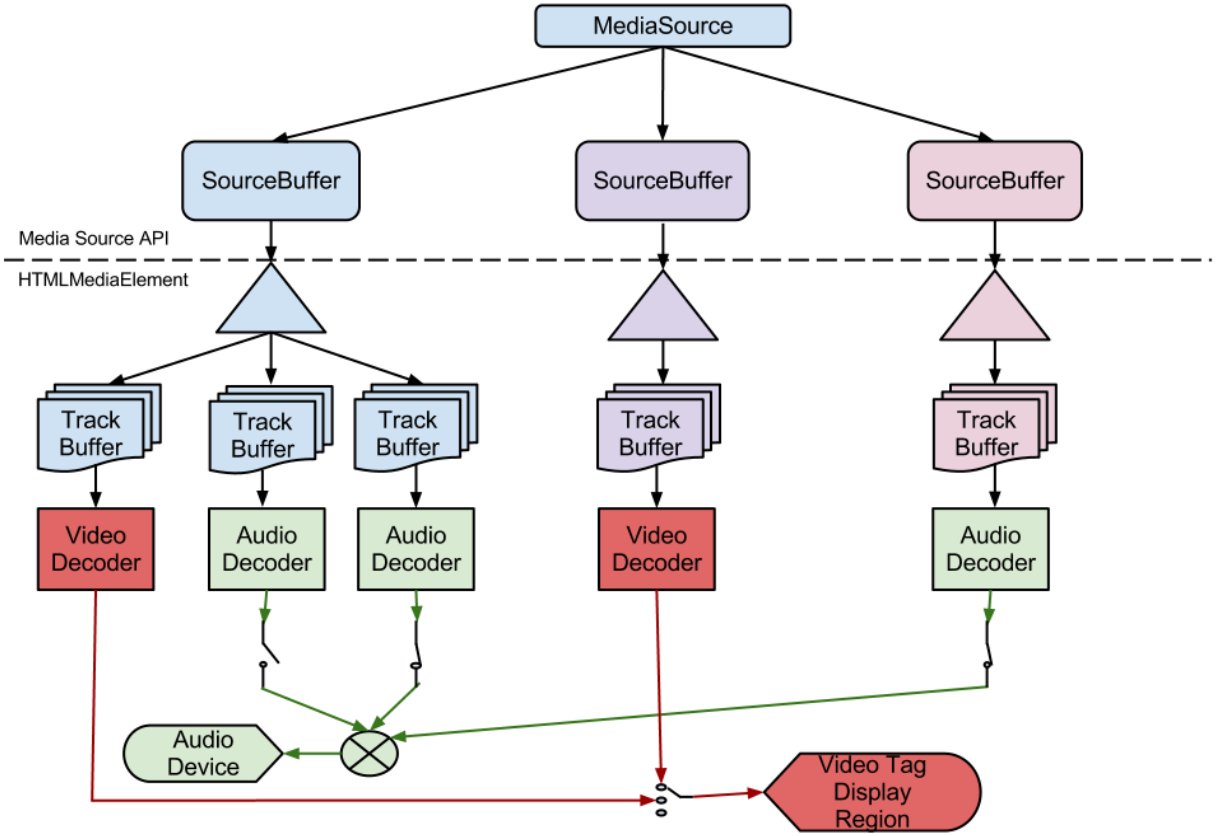
“Boxes” in ISOBMFF:



Fraunhofer FOKUS

STANDARDS - DASH&DRM
W3C MEDIA SOURCE EXTENSIONS

- Candidate Recommentation (31 March 2015)
- https://dvcs.w3.org/hg/html-media/raw-file/tip/media-source/media-source.html



Fraunhofer FOKUS

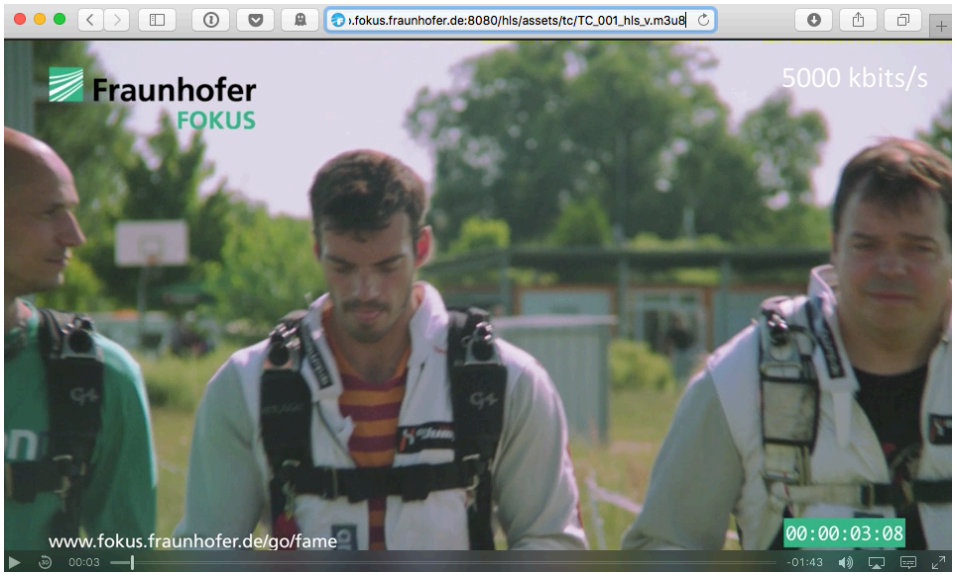
TYPES OF BROWSER-BASED DASH PLAYBACK

- Type 1: HTML5 <video>

```
<video id="video" controls width=1280 height=720
                src=”dash.mpd"></video>
```

- Type 2: HTML5 <video> + ABR API
- **Type 3: Media Source Extension (MSE)**

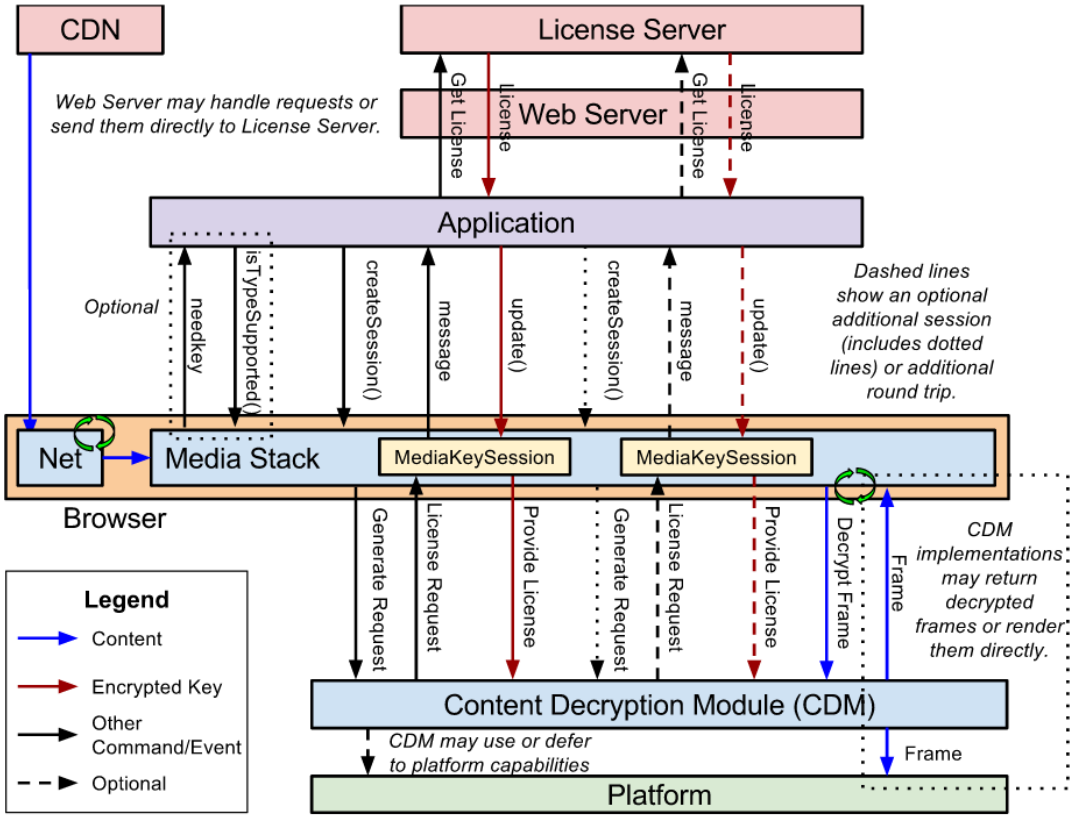
Source: http://blogs.windows.com/msedgedev/2015/07/02/moving-to-html5-premium-media/



Fraunhofer FOKUS

W3C ENCRYPTED MEDIA EXTENSIONS

– Working Draft: http://www.w3.org/TR/encrypted-media/ (31 March 2015)



BROWSER-BASED CONSUMPTION OF ENCRYPTED MEDIA

- Content:
  - Combination of ISO BMFF + Common Encryption (CENC)
  - CENC supports multiple DRM systems

- Browser-side:
  - Encrypted Media Extensions (EME)
  - Native Content Decryption Module
  - Handling of content exposed to JavaScript

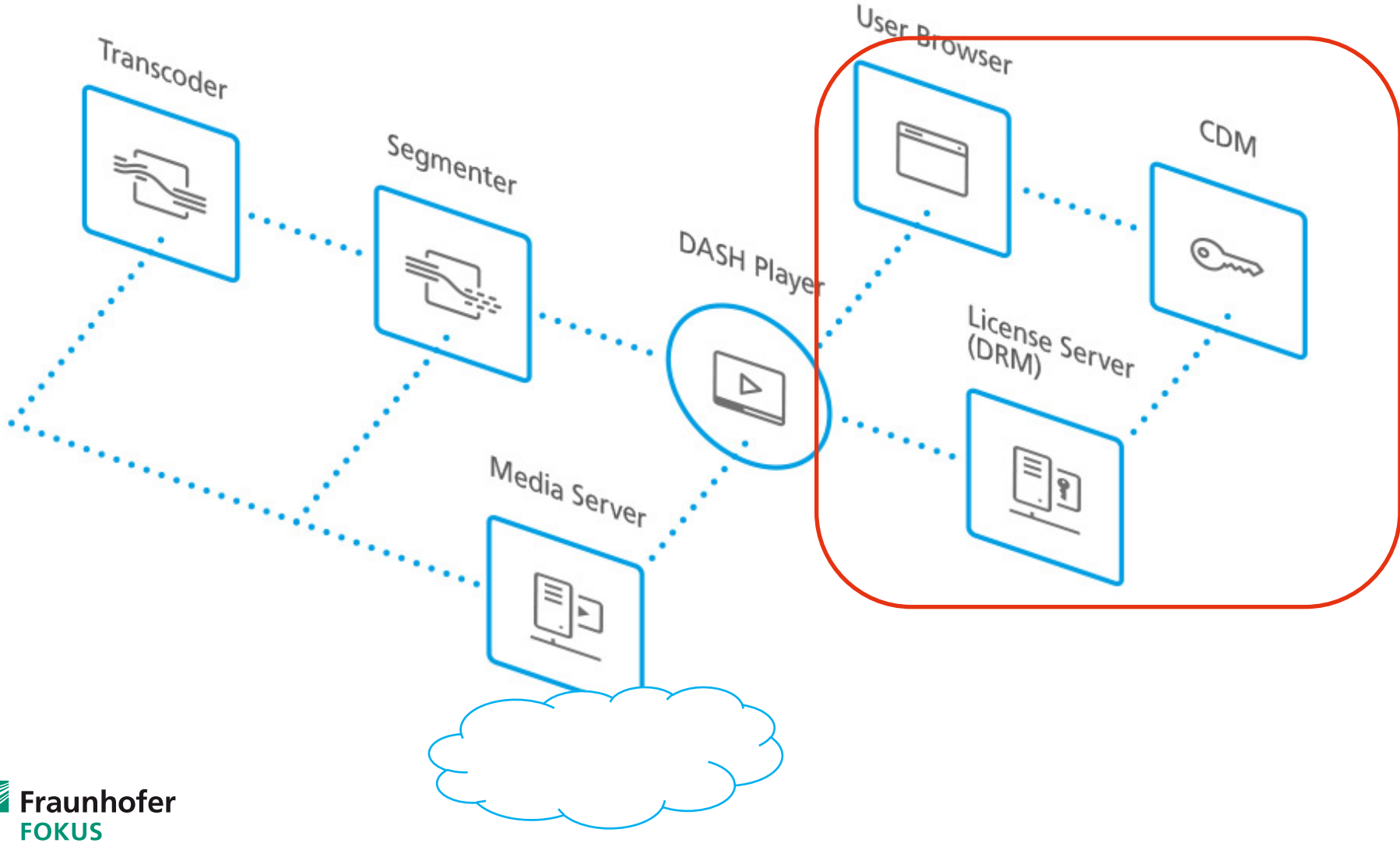
- MPEG-DASH supports encryption on content side
- On browser-side MSE+EME support encrypted MPEG-DASH

Fraunhofer FOKUS

Web & Media I

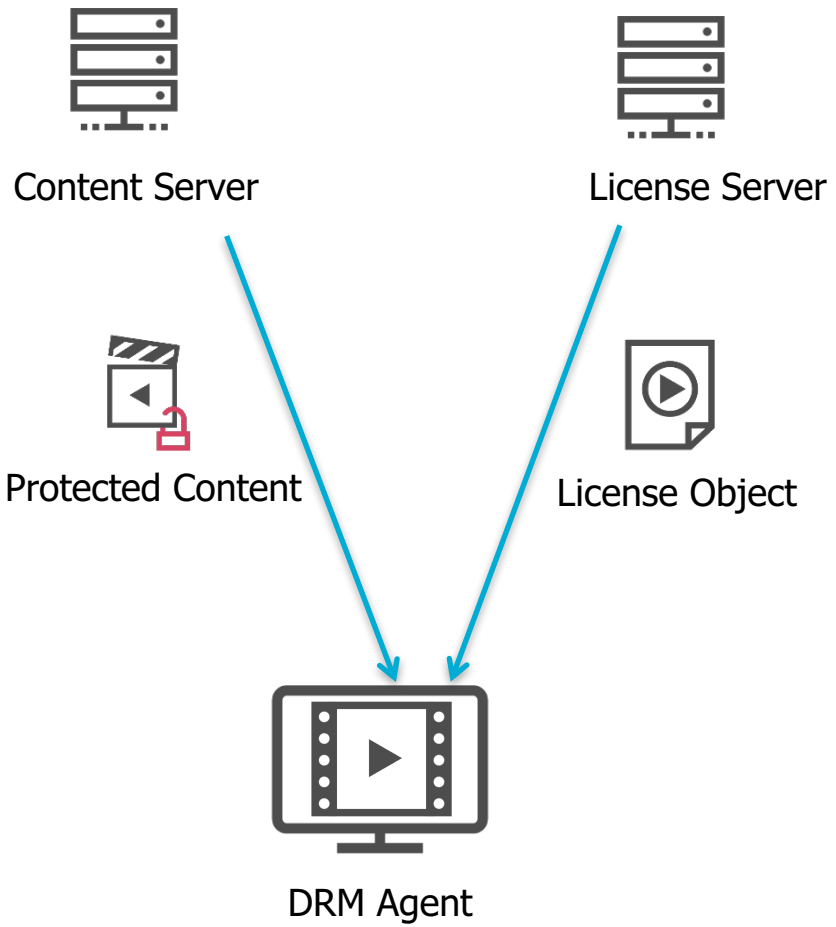
Digital Rights Management (DRM)

OVERVIEW



Fraunhofer FOKUS

GENERIC DRM ARCHITECTURE



Content Provider

User

Fraunhofer FOKUS

DRM

"We have Ph.D.'s here that know the stuff cold, and we don't believe it's possible to protect digital content." Steve Jobs, December 2003

"This is unethical." Ian Hickson, HTML5 editor, upon learning of the Netflix-Google-Microsoft Encrypted Media Extensions proposal - February 2012

"No one likes DRM as a user, wherever it crops up. It is worth thinking, though, about what it is we do not like about existing DRM-based systems". – Tim Berners-Lee, October 2013

"We have come to the point where Mozilla not implementing the W3C EME specification means that Firefox users have to switch to other browsers to watch content restricted by DRM ". – Andreas Gal, former Mozilla CTO, May 2014

Fraunhofer FOKUS

DRM

- Current DRM Systems
  - Microsoft Playready
  - Marlin
  - OMA DRM
  - Apple FairPlay
  - Adobe Access
  - Google Widevine
  - Many more, all proprietary

Fraunhofer FOKUS

MOVIELABS ENHANCED CONTENT PROTECTION

- Holywood studios specify requirements on premium UHD content:
  - Cryptography
  - Connection
  - Hack One, Only Hack One: Binding to Device, Software Diversity, Copy & Title Diversity
  - Revocation & Renewal
  - Output & Link Protection
  - Secure Computation Environment
  - Hardware Root of Trust
  - Watermarking
  - Breach Response
  - Certification

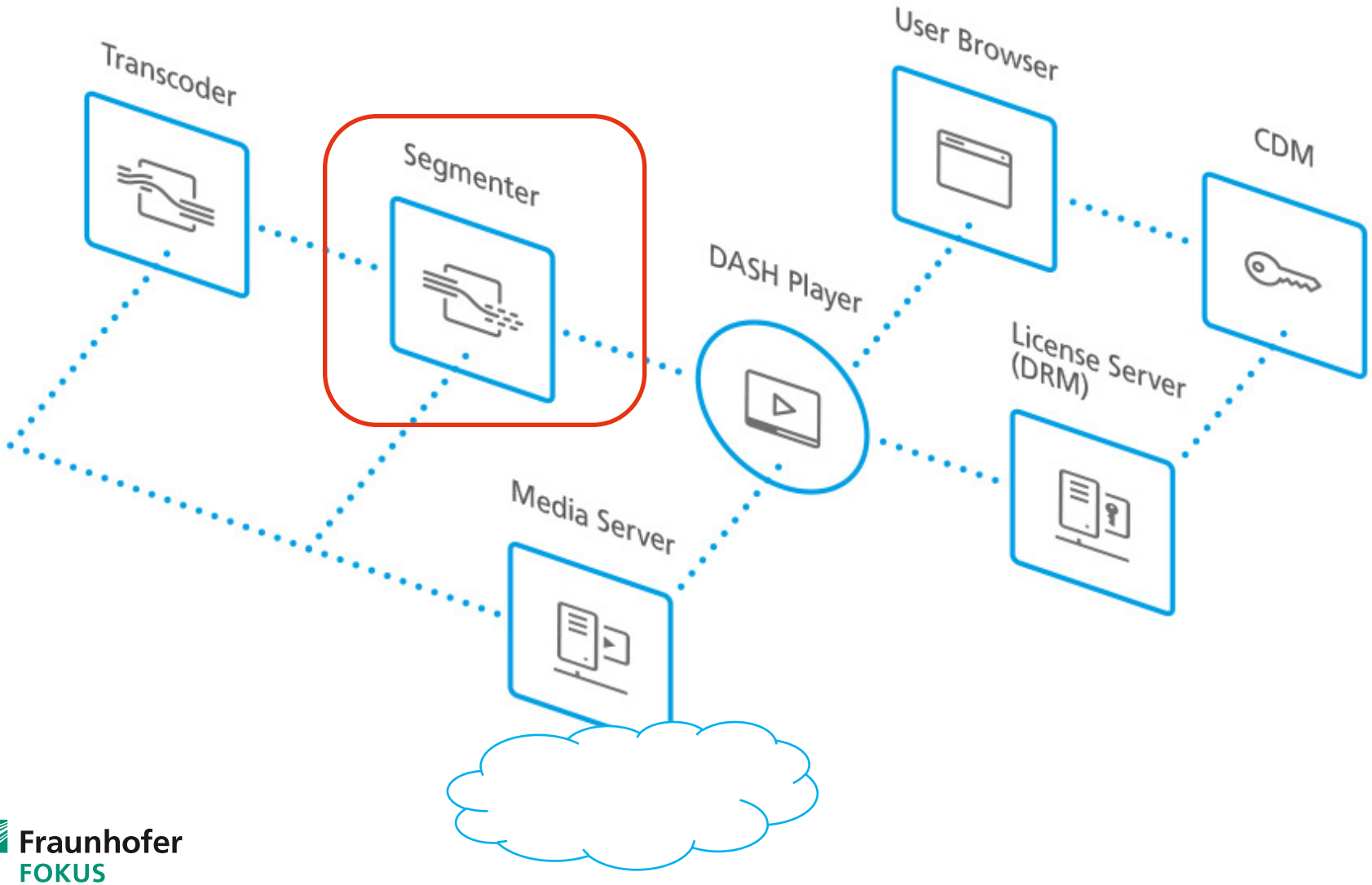
Source: http://www.movielabs.com/ngvideo/

Fraunhofer FOKUS

Web & Media I

Common Encryption (CENC)

OVERVIEW

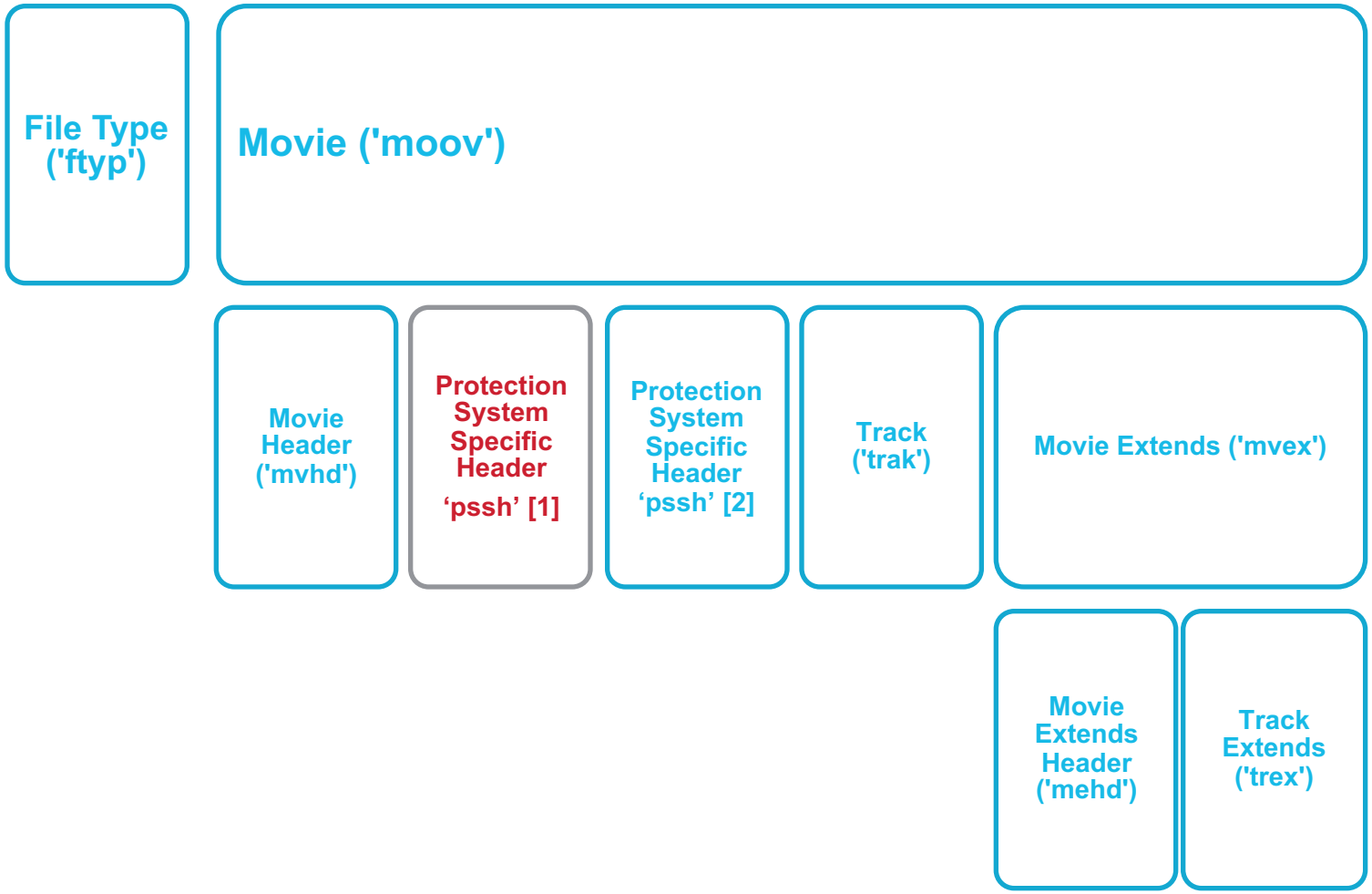


Fraunhofer FOKUS

COMMON ENCRYPTION (CENC)

- ISO/IEC 23007-1 (3rd edition) – Common encryption in ISO based media file format files
- Protection schemes: ’cenc’, ’cbc1’, ‘cens’, ‘cbcs’
- Common encryption means the same short fragment of video can be decrypted and decoded by devices using different DRMs.
- Improved encoding, network cache (origin vs. edge server) and CDN efficiencies

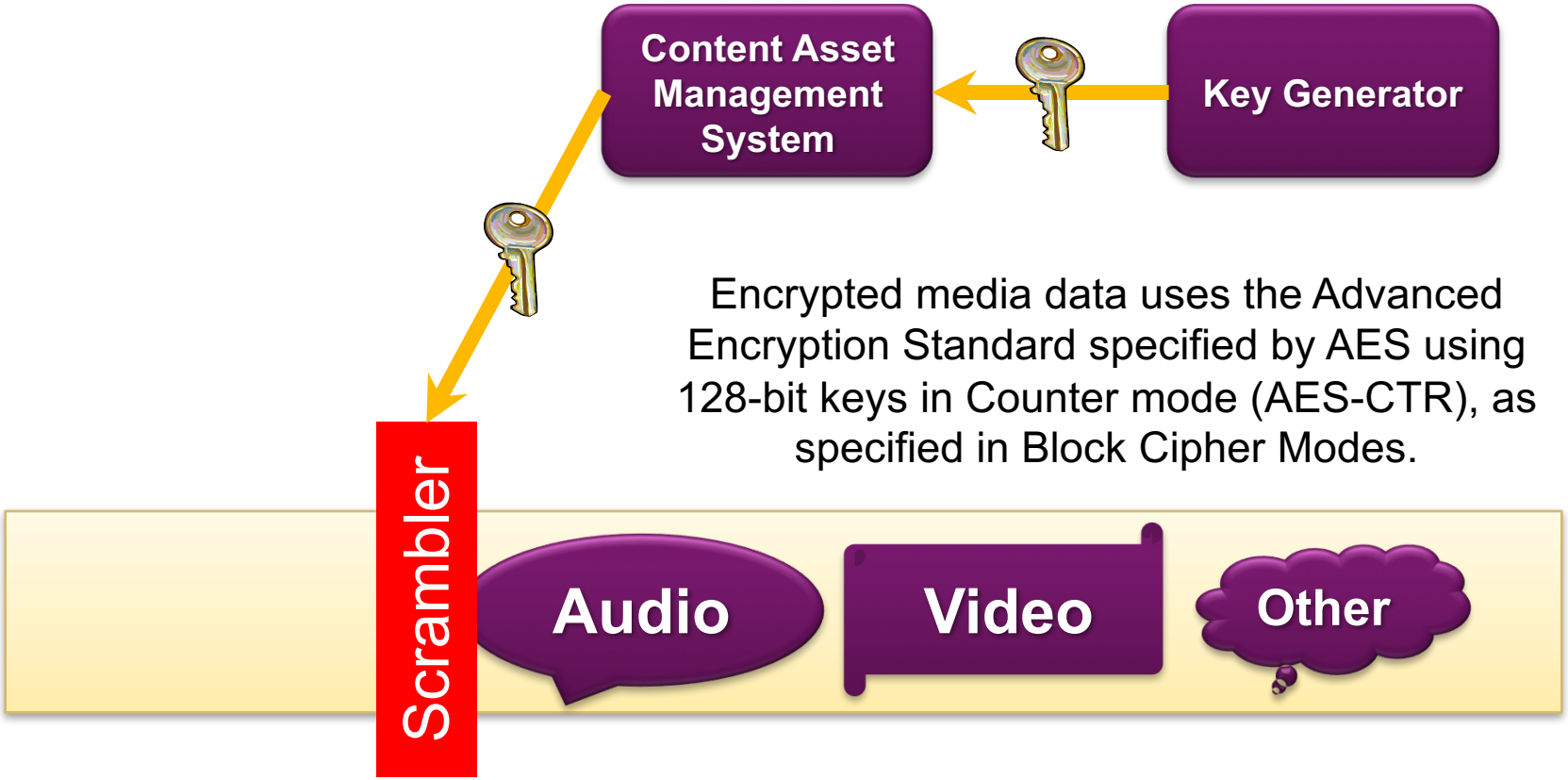
PROTECTION SYSTEM HEADER BOX



Fraunhofer FOKUS

MEDIA CREATION (FILE OR STREAM)

COMMON FILE FORMAT ENCRYPTION



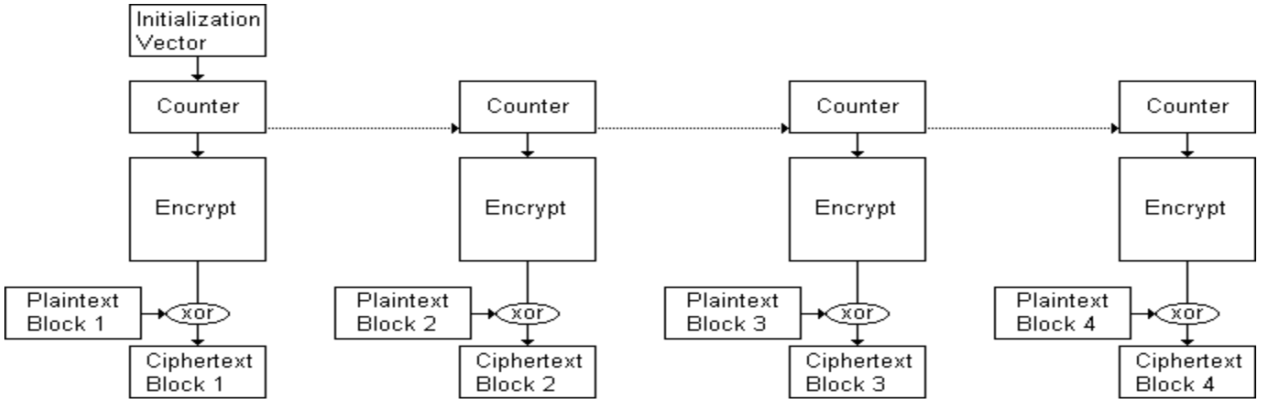
Fraunhofer FOKUS

ENCRYPTION

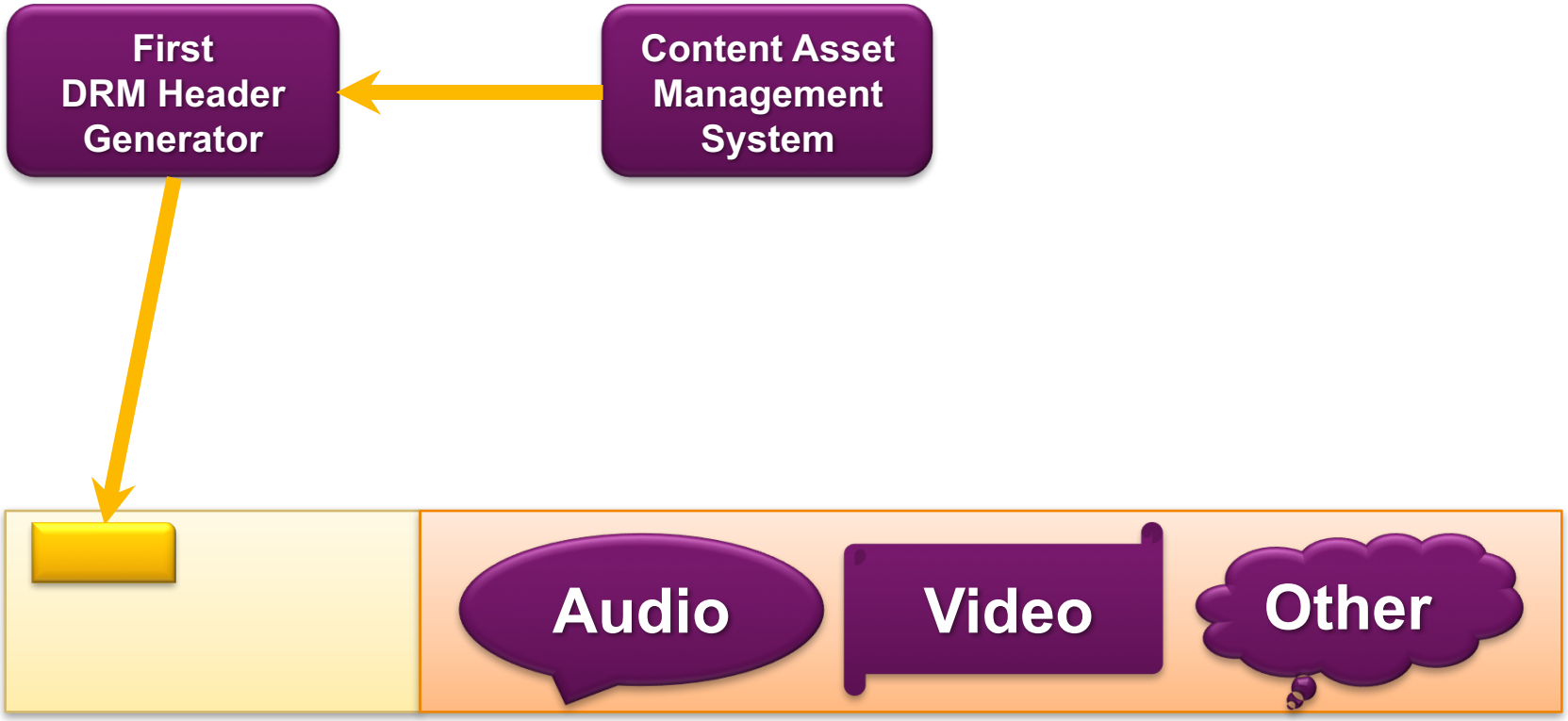
- Encrypted media data uses the Advanced Encryption Standard specified by AES using 128-bit keys in Counter mode (AES-CTR), as specified in Block Cipher Modes.

- Advanced Encryption Standard, Federal Information Processing Standards Publication 197, FIPS-197, http://www.nist.gov/

- Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A, http://www.nist.gov/

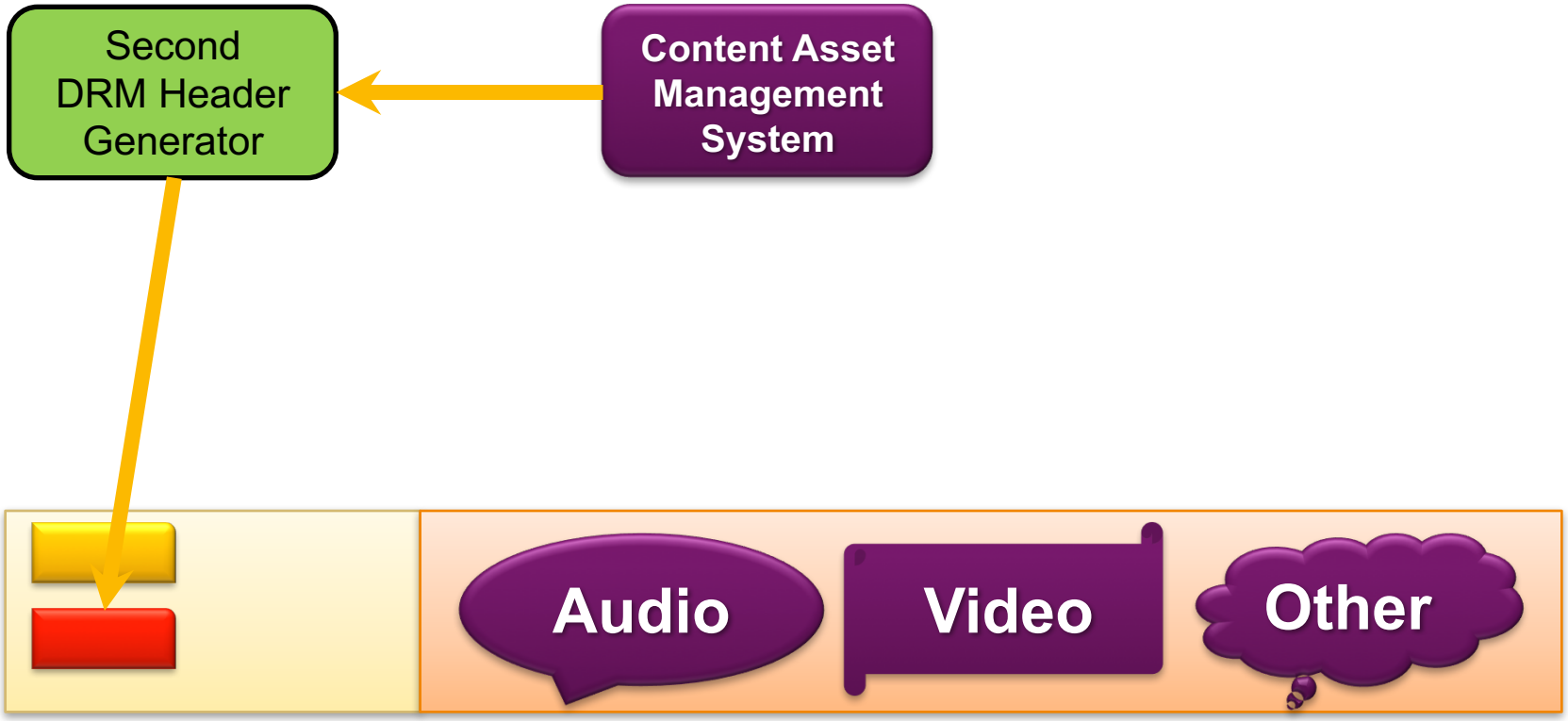


COMMON ENCRYPTION - HEADER GENERATION



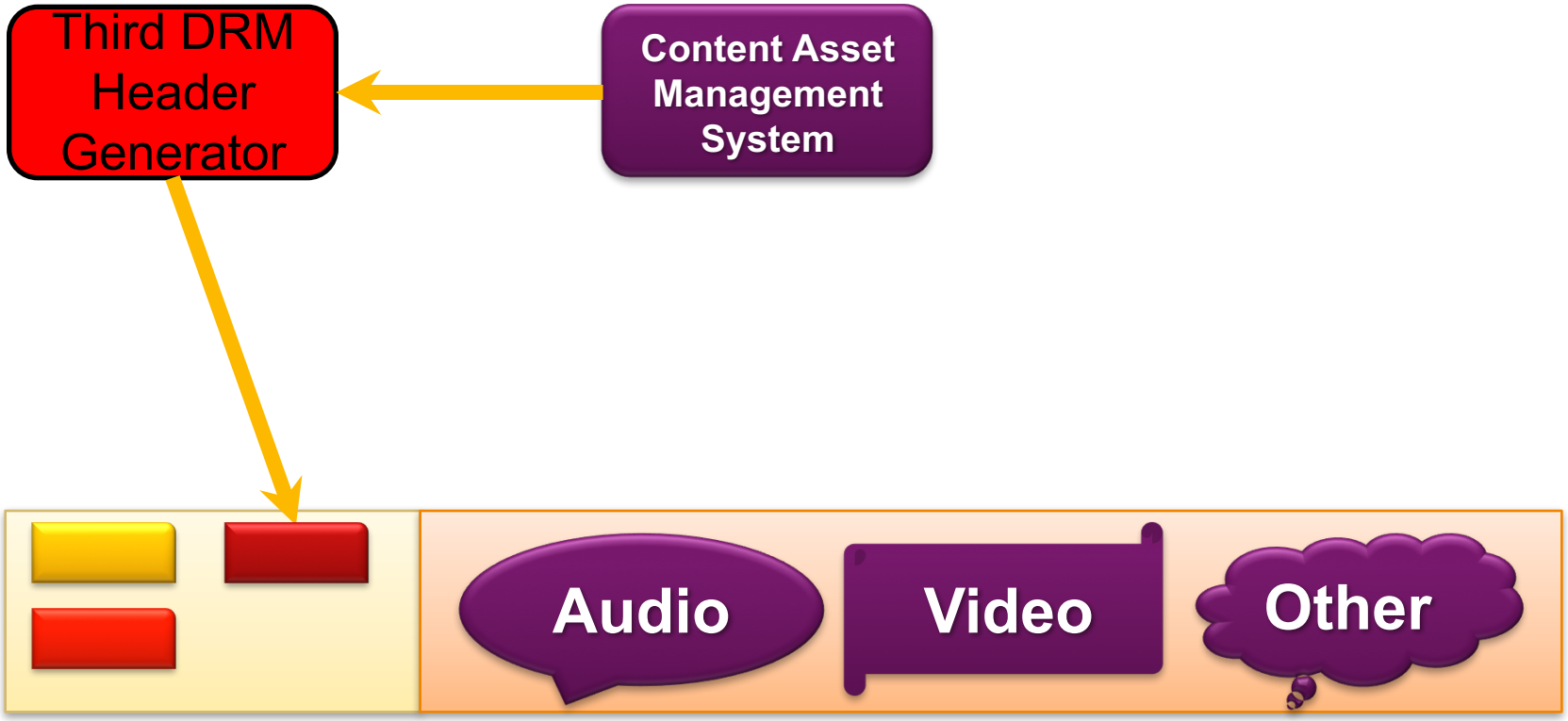
Fraunhofer FOKUS

COMMON ENCRYPTION - HEADER GENERATION



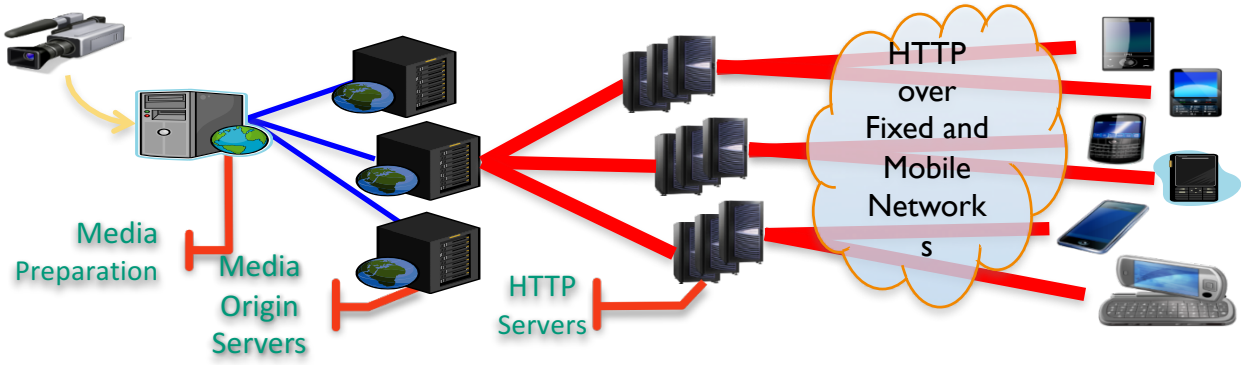
Fraunhofer FOKUS

CENC HEADER GENERATION



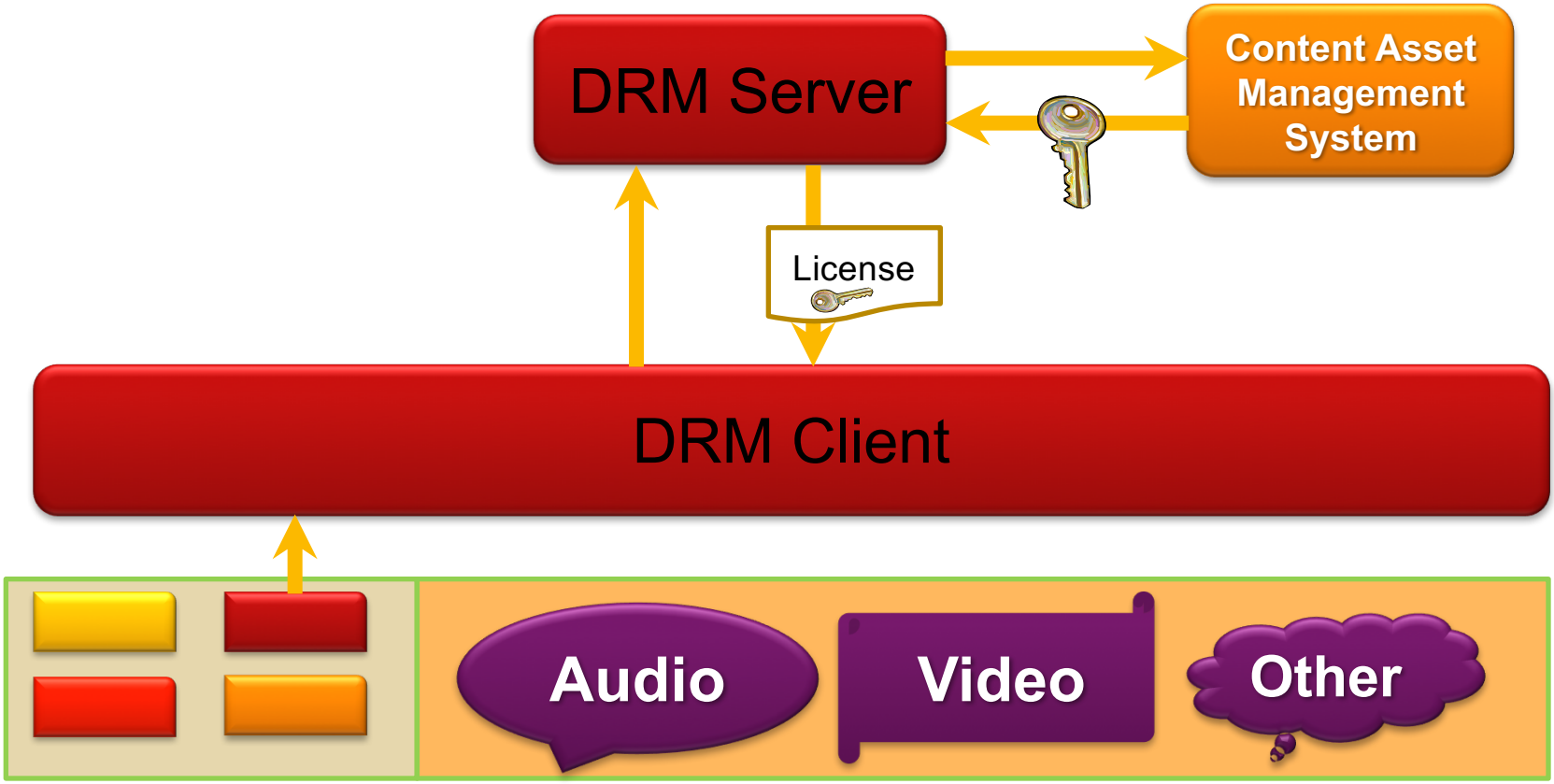
Fraunhofer FOKUS

TRANSMISSION



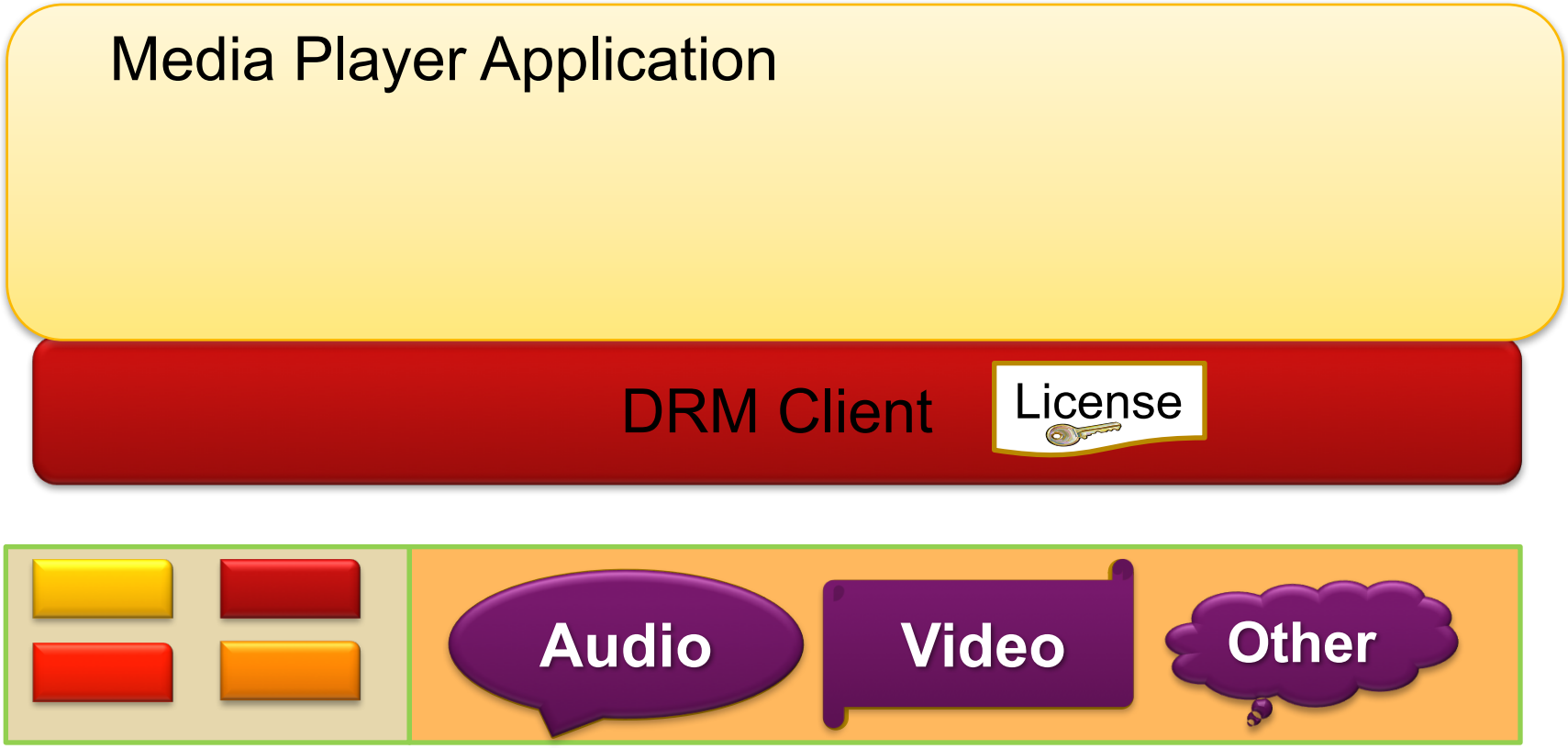
Fraunhofer FOKUS

DRM LICENSE RETRIEVAL



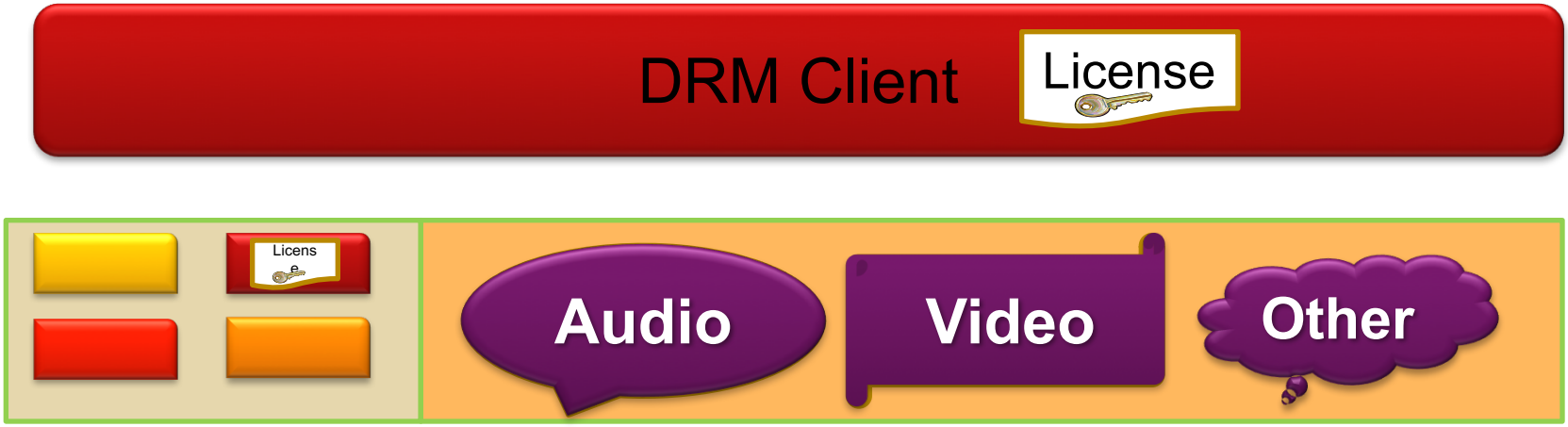
Fraunhofer FOKUS

DRM DECRYPTION



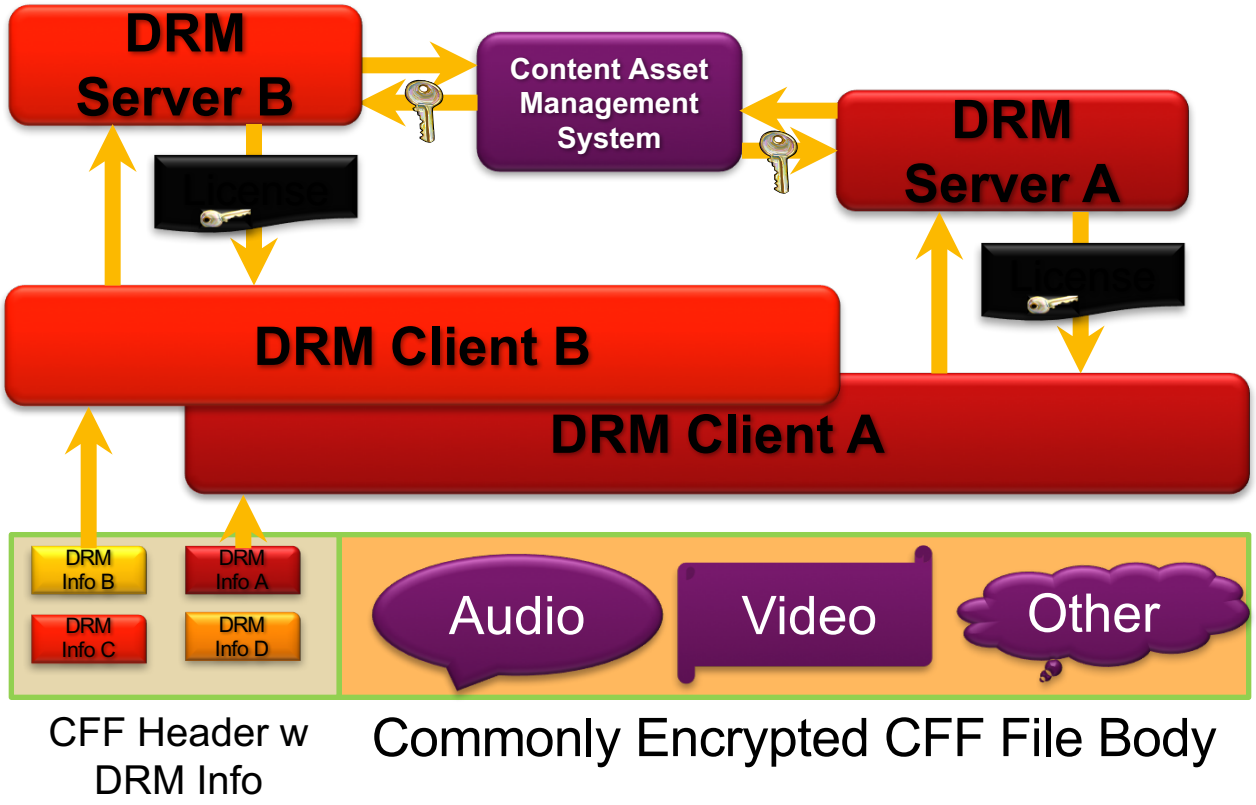
Fraunhofer FOKUS

DRM LICENSE EMBEDDING



Fraunhofer FOKUS

STANDARDS - DASH&DRM
MULTIPLE DRMS IN PARALLEL



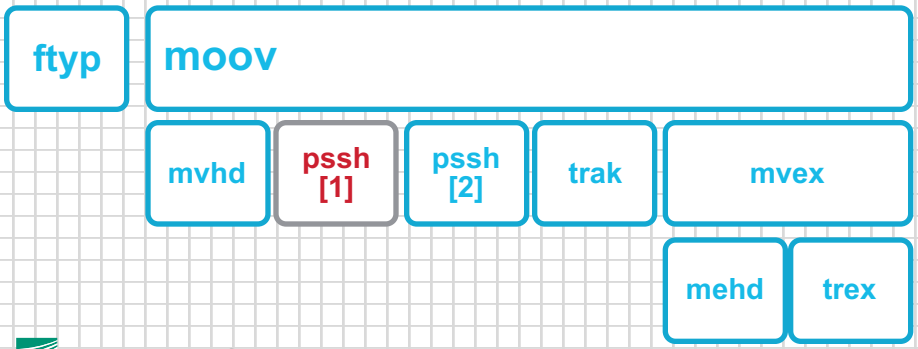
Fraunhofer FOKUS

EXAMPLE: CENC STREAM ANALYSIS

- CENC Defines new box named “pssh” (protection system specific header)
- This box contains DRM specific information like:
  - License acquisition URL
  - The unique DRM identifier UUID
  - Policies
  - Key Identifier (KID)
  - Provider name
  - Content ID

Setup

- Safari/OSX & Chrome/Linux with Web Inspector
- Download DASH Segments
- Isoviewer: https://code.google.com/p/mp4parser/ or http://thumb.co.il
- DRM identifiers: http://dashif.org/identifiers/protection



Fraunhofer FOKUS

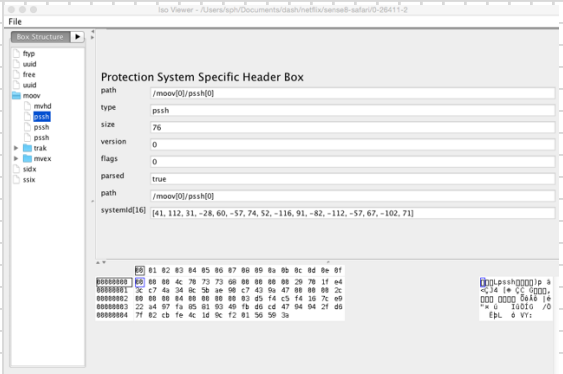
EXAMPLE: CENC STREAM ANALYSIS

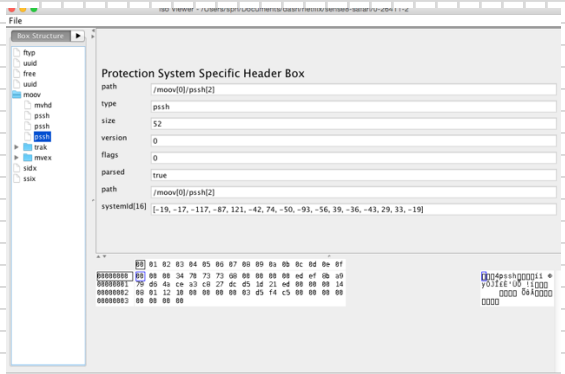
Which file format and DRM is Netflix using?

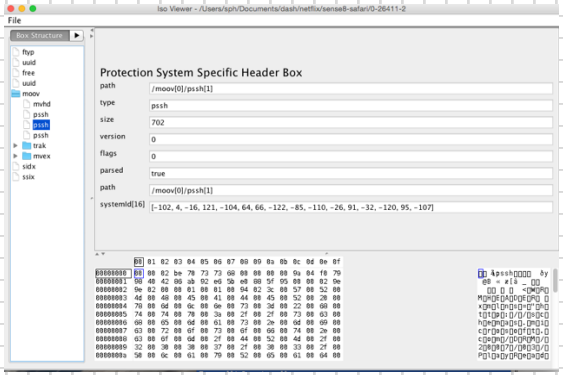
Streaming: DASH / ISOBMFF

DRM: Widevine, PlayReady, Fairplay

ISOViewer screenshots:





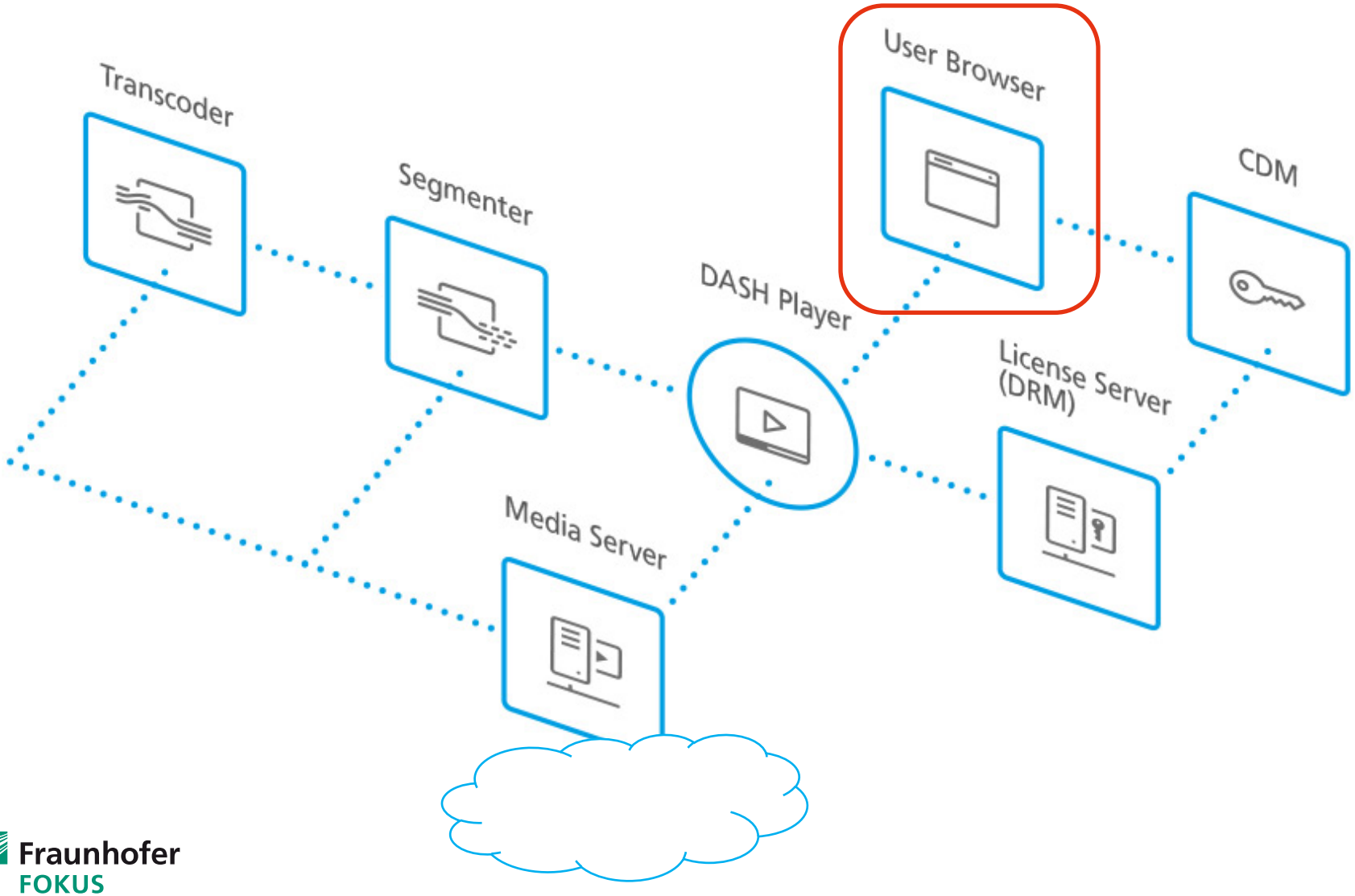


Fraunhofer FOKUS

Web & Media I

Encrypted Media Extension

OVERVIEW



Fraunhofer FOKUS

BROWSER-BASED CONSUMPTION OF ENCRYPTED MEDIA

- Content:
  - Combination of ISO BMFF + Common Encryption (CENC)
  - CENC supports multiple DRM systems

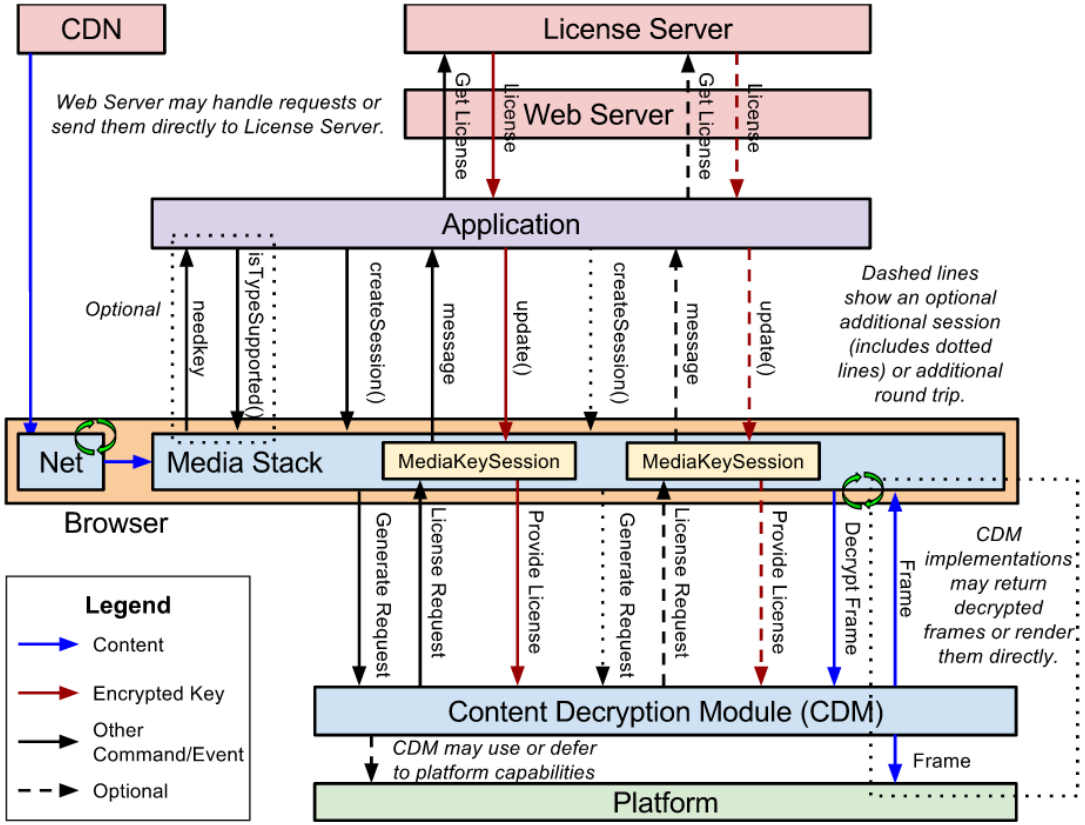
- Browser-side:
  - Encrypted Media Extensions (EME)
  - Native Content Decryption Module
  - Handling of content exposed to JavaScript

- MPEG-DASH supports encryption on content side
- On browser-side MSE+EME support encrypted MPEG-DASH

Fraunhofer FOKUS

W3C ENCRYPTED MEDIA EXTENSIONS

– Candidate Recommendation: https://www.w3.org/TR/encrypted-media/ (05 July 2016)



Fraunhofer FOKUS

W3C EME CODE EXAMPLE: ONNEEDKEY

```
<video src="foo.webm" autoplay onneedkey="handleKeyNeeded(event)"></video>

...

function handleKeyNeeded(event) {
  var video = event.target;
  if (!video.mediaKeys) {
    selectKeySystem();
    video.setMediaKeys(new MediaKeys(keySystem));
  }
  if (!video.mediaKeys) {
    throw "Could not create MediaKeys";
  }
  var keySession = video.mediaKeys.createSession(event.contentType,
      event.initData);
  if (!keySession) {
    throw "Could not create key session";
  }
  keySession.addEventListener("message", licenseRequestReady, false);
}
```

Entry point for EME

Fraunhofer FOKUS

W3C EME CODE EXAMPLE: SELECTING A SUPPORTED KEYSYSTEM

```
function selectKeySystem() {
  if (MediaKeys.isTypeSupported("com.example.somesystem",
      "video/webm; codecs='vp8, vorbis'")) {
    licenseUrl = "https://license.example.com/getkey";
    keySystem = "com.example.somesystem";
  } else if (MediaKeys.isTypeSupported("com.foobar",
      "video/webm; codecs='vp8, vorbis'")) {
    licenseUrl = "https://license.foobar.com/request";
    keySystem = "com.foobar";
  } else {
    throw "Key System not supported";
  }
}
```

Fraunhofer FOKUS

W3C EME CODE EXAMPLE: REQUESTING A LICENSE

```
...
keySession.addEventListener("message", licenseRequestReady, false);
...

function licenseRequestReady(event) {
  var keySession = event.target;
  var request = event.message;
  if (!request) {
    throw "Could not create license request";
  }
  var xmlhttp = new XMLHttpRequest();
  xmlhttp.open("POST", licenseUrl);
  xmlhttp.onreadystatechange = function () {
    if (xmlhttp.readyState === 4) {
      var license = new Uint8Array(xmlhttp.response);
      keySession.update(license); // playback can now begin
    }
  }
  xmlhttp.send(request);
}
```

Request a license from DRM server

Fraunhofer FOKUS

DEMO: MULTI-DRM PLAYBACK

Setup

- DASH+CENC (PR, WV, ClearKey) content
- Playback in dash.js (using MSE/EME) with keysystem selection
- EME instrumentation
- Chrome/Edge/Firefox compatible

Web & Media I

Reaching Streaming Devices

DRM SUPPORT ON DESKTOP WEB BROWSER

Desktop Browser	Platform	EME/CDM	Flash Player/ Primetime	NPAPI/ Silverlight 5
Chrome	Win	Widevine	(Yes)	No
	OSX		(Yes)	No
	Linux		(Yes)	No
Firefox	Win	Widevine, Adobe	Yes	Yes
	OSX		Yes	Yes
	Linux		(Yes)	Yes
Safari	> OSX Yosemite	(Fairplay)	Yes	Yes
	< OSX Yosemite	No	Yes	Yes
IE/Edge	< Win 7	No	Yes	Yes
	Win 10	PlayReady	Yes	No

DRM SUPPORT ON MOBILE

Mobile Platform	HTML5	Native App / DRM
iOS	No MSE/EME HLS (AES-128 CBC) via <video>	Native SDK and WebView: FairPlay
		3rd Party Player SDKs – almost any DRM/Streaming is possible (PlayReady, Widevine, Verimatrix, VisualOn, Authentec, Castlabs, Discretix, Irdeto, NDS, Saffron, etc.)
Android	MSE/EME	Native + Android SDK (MediaDRM APIs) - (Widevine + OMA v2)
		Native + WebView with Widevine
		3rd Party Player SDKs - almost any DRM is possible; any streaming format
Windows 10 Mobile	MSE/EME	WebViews/Hosted Web Apps with PlayReady

DRM SUPPORT ON TV/ GAME COSOLES

Platform	MSE/EME (DASH)	DRM
HbbTV 1.5/2.0	No 2.0.1 supports EME	TNT 2.0: Marlin/ PlayReady
Smart TV Alliance	optional	PlayReady (conditional-mandatory)/ Widevine (optional); Smooth (mandatory), DASH (optional)
Samsung (SDK 1.4)	Yes	PlayReady, Widevine, Verimatrix; DASH, HLS, Smooth
FireTV	No	VisualOn SDK + PlayReady (TrustZone); HLS/ DASH/ Smooth
Chromecast	Yes	Dash + PlayReady/ Widevine; Smooth + PlayReady HLS + AES
AppleTV	No	HLS + Fairplay
RDK	Yes (OCDM)	PlayReady, Adobe Access
AndroidTV	For Google devices – see Android mobile, difference only in Security Levels	

Platform	Web Browser (MSE/EME)	Native DRM
XBox	Yes (as Win10 Hosted App)	PlayReady
PS	No	PlayReady(?), Marlin

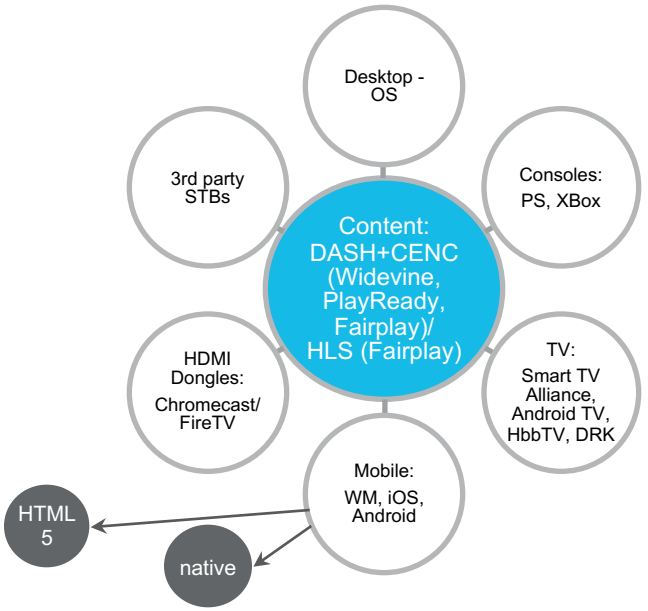
Fraunhofer FOKUS

STREAMING FORMAT FROM DRM PERSPECTIVE

How can we address different devices classes today?

- What‘s on the market?
  - SmoothStreaming, HDS
  - HLS + Fairplay
  - DASH + CENC
- Can we choose one technology?
  - No, it is not possible to address the variety of different device classes with one streaming standard.

- With the support of both streaming formats **HLS + Fairplay and DASH + CENC (Widevine, PlayReady)** all the device classes available on the market can be addressed

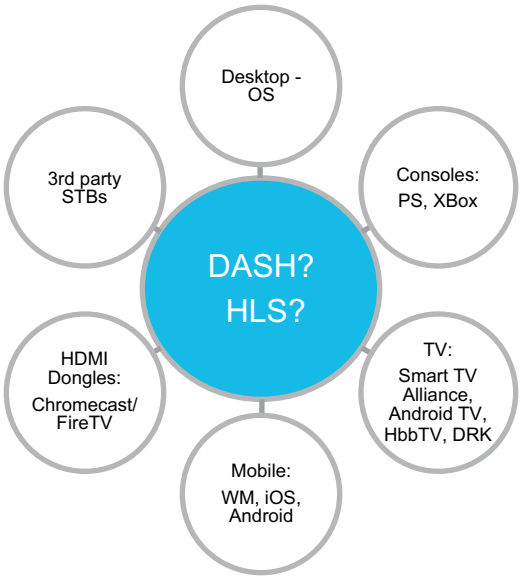


Fraunhofer FOKUS

WHY NOT A SINGLE STREAMING FORMAT?

Why not only DASH or HLS?

- Why not only DASH?
  → App Store Review Guidelines document for video streaming content over a cellular network:
  9.4 Video streaming content over a cellular network longer than 10 minutes must use HTTP Live Streaming and include a baseline 192 kbps or lower HTTP Live stream
- Why not only HLS?
  → we won‘t be able to address all other devices
- What about legacy streaming?
  → Smooth to DASH client-side converting is possible
  → HLS to DASH client-side converting is not possible due to DRM → both streaming formats are needed



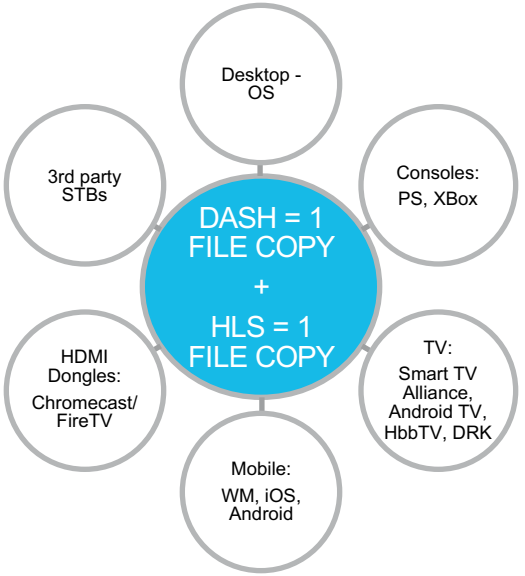
HOW MANY PHYSICAL FILE COPIES?

DASH and HLS

Streaming	File Format	Encryption
DASH	ISOBMFF	‘cenc’ (AES-CTR)

Streaming	File Format	Encryption
HLS	MPEG2TS	Sample-AES (AES-CBC)
HLS	ISOBMFF	‘cbcs’ (AES-CBC)

- Summary
  - 2 physical files encrypted with AES-CTR and AES-CBC
  - If only 1 encryption scheme
    → CDN cache efficiency



TRANSCODING ON THE CLIENT

Legacy (SmoothStreaming) and HLS to MPEG DASH

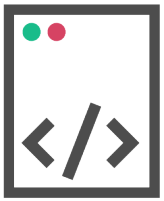
- Smooth with PIFF encryption can be transcoded on the fly to DASH with CENC on the client-side
  - SMOOTH+PIFF → DASH+CENC on the client
- HLS-Fairplay can not be transcoded to DASH-CENC on the client-side due to different AES encryption
  - HLS+Fairplay → DASH+CENC on the client
- Open source MSE players:
  - Hasplayer (Smooth/HLS to DASH)
  - Hls.js (HLS to DASH for unprotected content)

Web & Media II

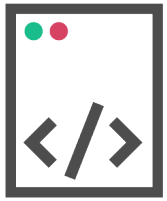
Live Streaming

MPEG-DASH GENERATION

- In: Source file to be DASH'd



- Transcoding of source into different bitrates



- Segmentation of different bitrates into DASH format. Optional application of DRM protection

- Out: DASH content, clear or protected

Fraunhofer FOKUS

MPEG-DASH LIVE:STATE OF THE ART

- Live Transcoding with RasbperryPis
  - Using FAMIUM tools from local camera
  - Each Pi transcodes 1 A/V bitrate

  → 20-30 seconds latency

- Other references:
  - Heise World Cup 2014 comparison
    - Adaptive Streaming latency > 30-90s
  - Zattoo Whitepaper

Fraunhofer FOKUS

MPEG-DASH LIVE LOW-LATENCY

- In general:
  - HTTP Streaming does not have quality assurance (in contrast to broadcast or managed networks)
- What is causing latency?
  - Video encoding:
    - segment length
    - # of a/v bitrates
  - Player buffering behavior:
    - buffer size
    - parallel vs. sequential
    - DASH MPD (minBufferTime, availabilityStartTime)
  - Transport:
    - CDN, caching
    - TCP-IP

Fraunhofer FOKUS

MPEG-DASH LIVE LOW-LATENCY

- Solutions:
  - Optimizations for Video encoding, player buffering and transport possible, but limited
    - Smaller segments and file format changes to improve coding efficiency
    - Tuning player buffering algorithms (startup, buffer size, segment fetching, representation switching)
  - Alternative and new transport protocols in consideration:
    - HTTP/2 PUSH, SSE
    - WebSockets, WebRTC
    - Multiple TCP

CONTACT

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
www.fokus.fraunhofer.de

Stefan Pham
Project Manager R&D
stefan.pham@fokus.fraunhofer.de
Phone +49 (0)30 3463-7103

THANKS FOR YOUR ATTENTION

Fraunhofer FOKUS