Fraunhofer FOKUS
Institut für Offene Kommunikationssysteme

Advanced Media Streaming

Advanced Web Technologies | Open Distributed Systems

Stefan Pham

Nov 6th, 2023

Fraunhofer FOKUS

Schedule

No	Week	Date	Topic
1	42	16.10.2023	Introduction and Framework
2	43	23.10.2023	Web Technologies Basics / Media Entertainment for the Web
3	44	30.10.2023	Foundations of Media Streaming
4	45	06.11.2023	Advanced Media Streaming
5	46	13.11.2023	Multiscreen Technologies and Standards
6	47	20.11.2023	HbbTV and Smart TV
7	48	27.11.2023	Media Players - dash.js, Exoplayer
8	49	04.12.2023	Dynamic Advertisement
9	50	11.12.2023	Context-Aware Media Streaming & Encoding
	51	18.12.2023	Holiday break
	52	25.12.2023	Holiday break
	1	01.01.2024	Holiday break
10	2	08.01.2024	Media Delivery in 5G Networks (1)
11	3	15.01.2024	Media Delivery in 5G Networks (2)
12	4	22.01.2024	Metaverse Platforms and Technologies
13	5	29.01.2024	Securing Content-Provenance and Authenticity
14	6	05.02.2024	Interoperable Web-supported Learning Technologies
15	7	12.02.2024	Exercise and Test Preparation
16	8	19.02.2024	Written Test (60min) first slot

Agenda

1. Intro
2. DRM Standards
3. Watermarking
4. Cross-Platform Streaming
5. Streaming Analytics

Fraunhofer FOKUS

Intro

Fraunhofer FOKUS

OTT Delivery: Tech to understand

ABR – Adaptive Bitrate

DASH – Dynamic Adaptive Streaming over HTTP for live and on demand video; MPEG standard

HLS – HTTP Live Streaming for live and on demand video by Apple

MSS – Microsoft Smooth Streaming

CMAF – Common Media Application Format for HLS and DASH

IMSC – Internet Media Subtitles and Captions

CENC – Common Encryption for many DRM & delivery channels

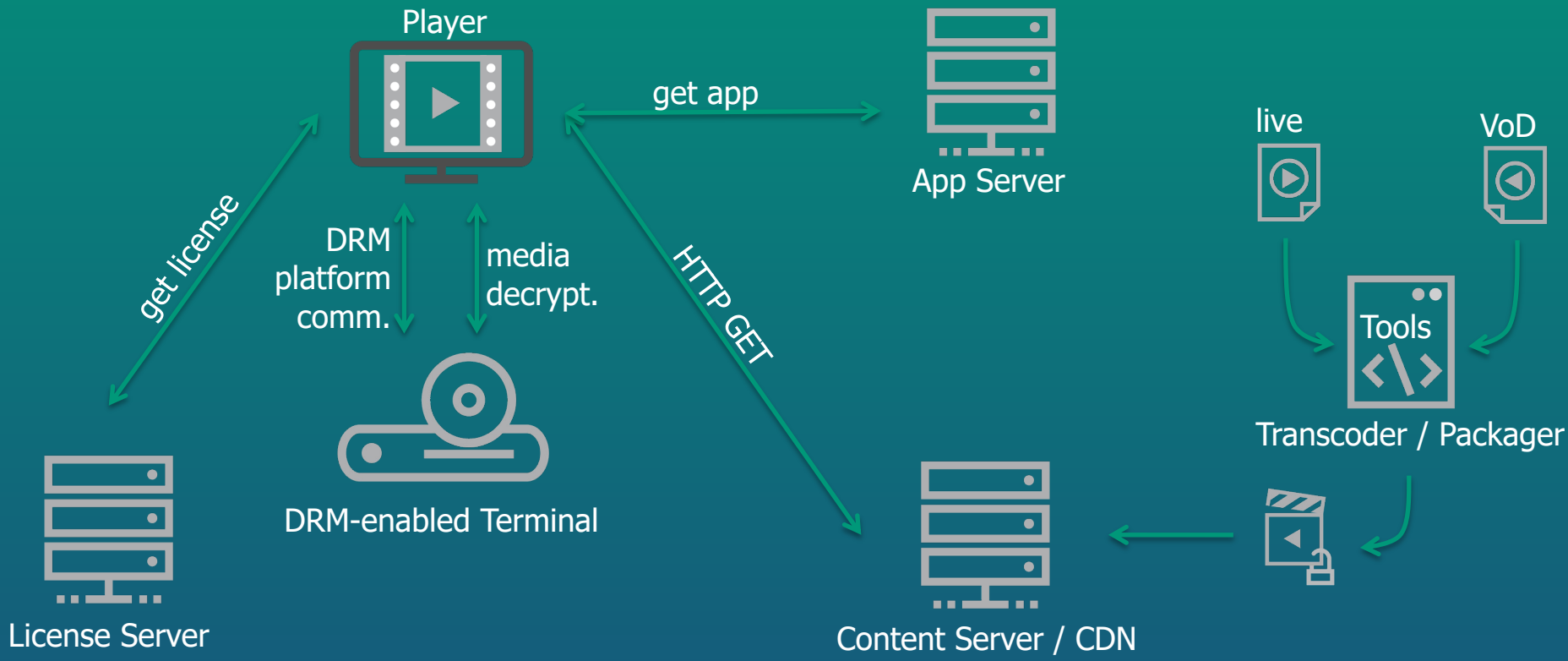
MSE – Media Source Extension to trick-function HTML5 video-objects via JavaScript (control AV media streams)

EME – 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

CPIX – Content Protection Information Exchange Format - standardizes the way entities involved in the content creation workflow exchange protection information

Media Streaming Workflow



Fraunhofer FOKUS

OTT ABR Streaming – Mission accomplished?

- Encoding ladders are mainly static, but there is a trend towards dynamic/context-aware ladders
- OTT ABR Streaming with DASH and HLS is used everywhere
- CMAF has become the standard container format
- LL-HLS and LL-DASH are maturing and will be used for big sports events

Status quo:

Different device platforms & interoperability – *how to reach them all? Best practices?*

Other factors:

– ***Monetization*** **(DAI),**
– ***Regulatory*** **(DRM, watermarking),**
– ***Quality*** **(UHD, 8K, HDR, Codec evolution),**
– ***Analytics*** **(streaming metrics, troubleshooting),**
– ***UX*** **(AR/VR, 360°, interactivity, 6DoF)**
– ***Transport (HTTP/3, 5G Broadcast)***

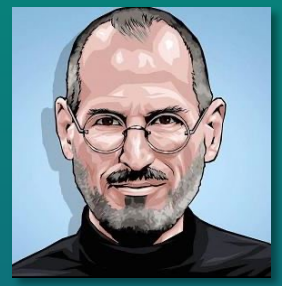
DRM Standards

Fraunhofer FOKUS

DRM, Commercial Media and the Internet

"Digital files cannot be made uncopyable, any more than water can be made not wet.“ Bruce Schneier, May 2001

“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*



“If we’re still talking about DRM in five years, please take me out and shoot me.” eMusic CEO David Pakman, February 2007

“This is unethical.” Ian Hickson, HTML5 editor, upon learning of the Netflix-Google-Microsoft Encrypted Media Extensions proposal - February 2012 (5 years later)

Source: John Simmons

Today’s DRM Systems

Microsoft PlayReady	Google Widevine	Apple FairPlay	Huawei WisePlay
Microsoft | PlayReady®	WIDEVINE	FairPlay	WisePlay

DRM Standards - DRM Media Streaming Stack

Multi-DRM

- Content Protection Information Exchange Format (CPIX)

Encryption

- Common Encryption (CENC)

Packaging

- Common Media Application Format (CMAF)
  - Dynamic Adaptive Streaming over HTTP (DASH)
  - HTTP Live Streaming (HLS)

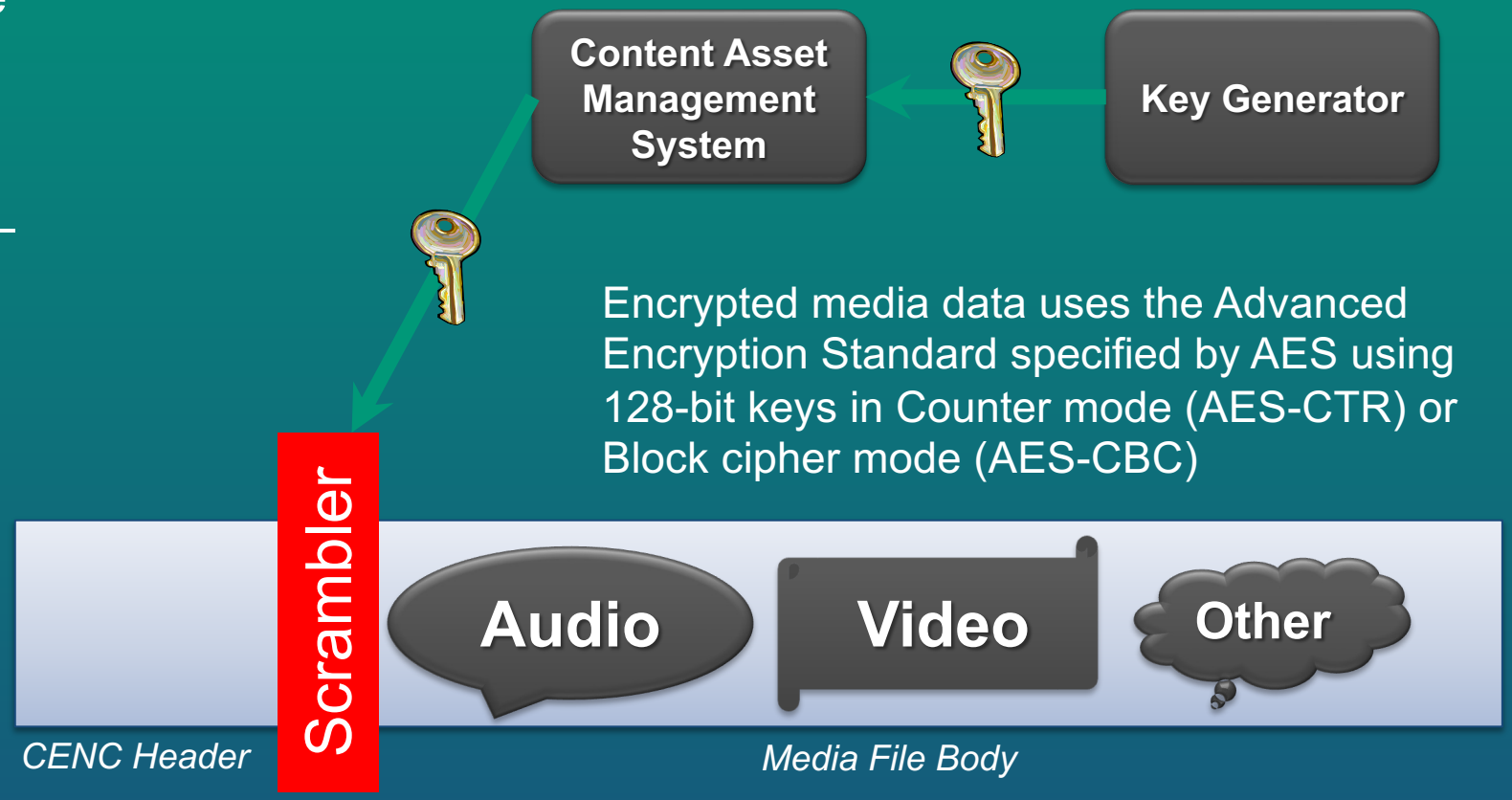
Playback

- dash.js with W3C Media Source Extensions (MSE) / Encrypted Media Extensions (EME)
- AVFoundation (iOS)
- ExoPlayer (Android)

Fraunhofer FOKUS

DRM Standards - Common Encryption (CENC)

- Common encryption means the same video can be decrypted and decoded by devices using different DRMs.
- ISO/IEC 23007-1 (3rd edition) – Common encryption in ISO based media file format files
- Protection schemes: ’cenc’, ’cbc1’, ‘cens’, ‘cbcs’

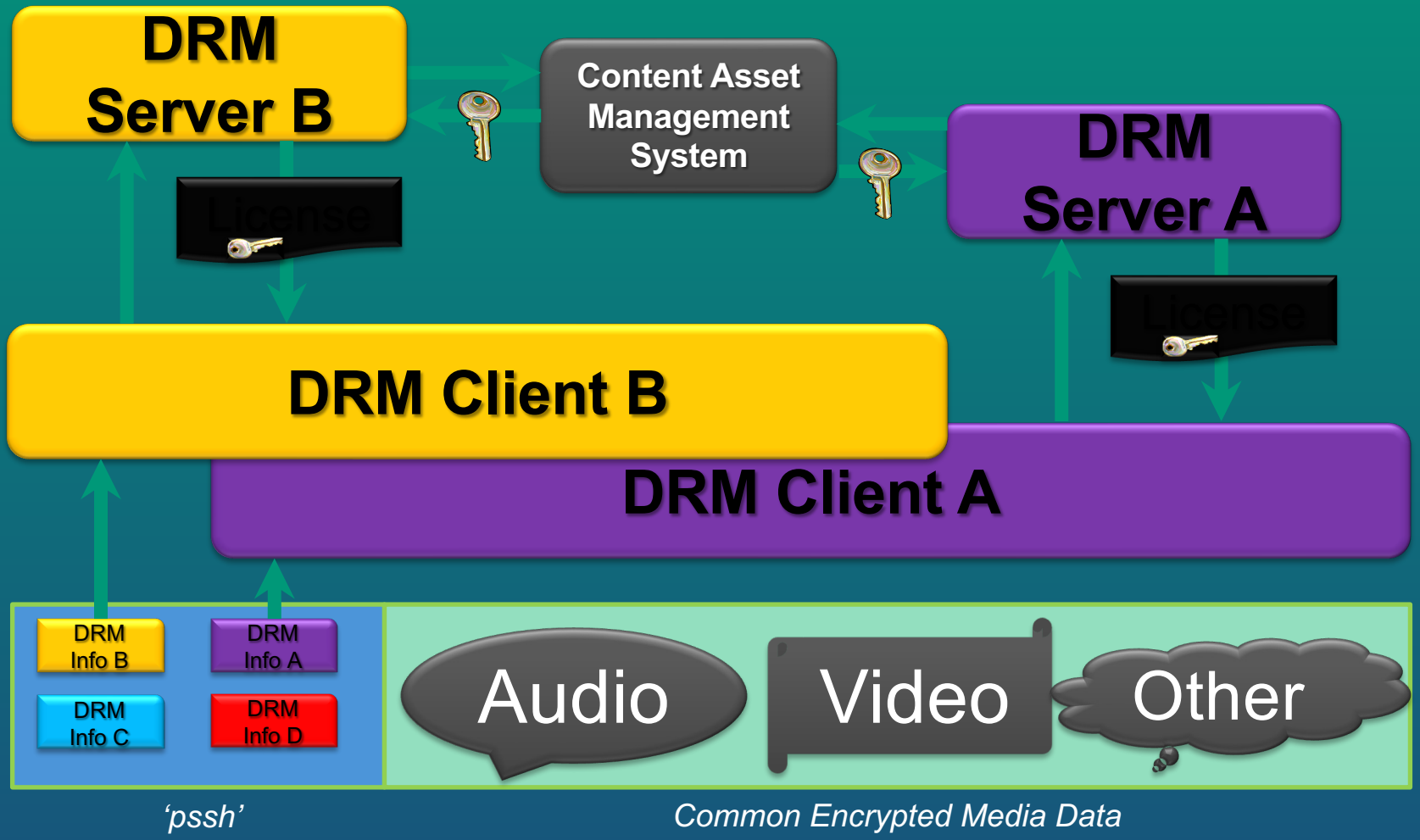


	Full sample encryption	Pattern encryption
AESCTR mode	‘cenc’	‘cens’
AESCBC mode	‘cbc1’	‘cbcs’

Source: https://learn.microsoft.com/de-de/playready/packaging/content-encryption-modes

Fraunhofer FOKUS

DRM Standards - Multi-DRM with CENC



Fraunhofer FOKUS

DRM Standards - Signalling DRM in DASH MPDs

Fraunhofer FOKUS

DRM Standards - Signalling DRM in HLS Playlists

- **EXT-X-SESSION-KEY** enables pre-fetching in the Primary Playlist
- **EXT-X-KEY** methods can be:
  - NONE
  - AES-128 (complete segment encryption)
  - SAMPLE-AES (typically ‘cbcs’ with CMAF)

Fraunhofer FOKUS

DRM Standards - Signalling DRM in ISOBMFF Init Segments

Fraunhofer FOKUS

DRM Standards - DRM signalling priority

From DASH-IF IOP (Content Protection and Security):

- **„cenc:pssh information in the MPD** allows faster parsing, earlier access, identification of duplicate license requests”
- “**’pssh’ boxes in Initialization Segments are not recommended** because they trigger a license request each time an Initialization Segment is processed in a Web browser for each Representation and bitrate switch.”
- “In the case where the ‘pssh‘ box element is present in the MPD and in the Initialization Segment, the ‘pssh‘ box element in the **MPD SHALL take precedence**"

Fraunhofer FOKUS

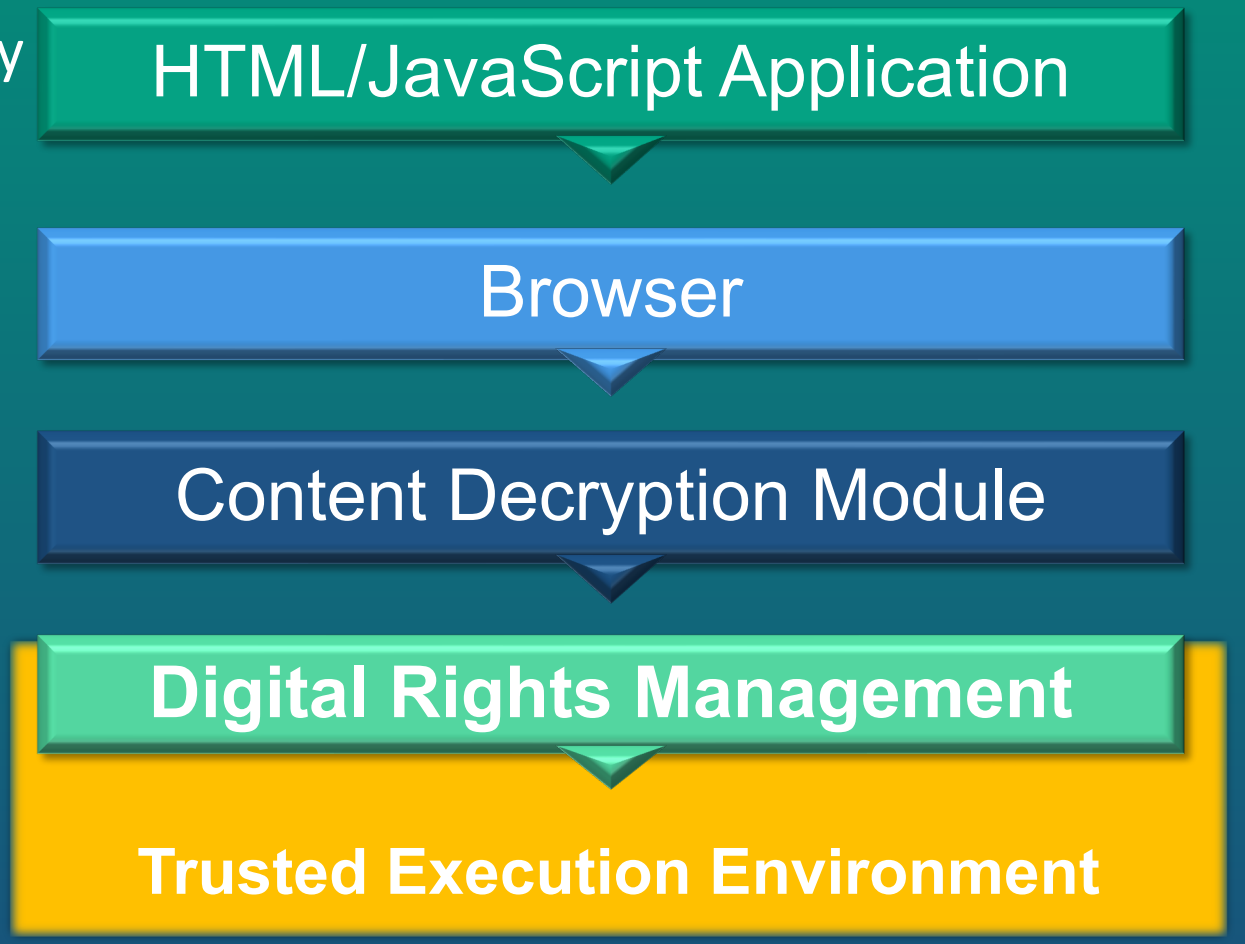
DRM Standards - The Web, EME and Enhanced Content Protection

The **HTML/JS** app is portable but not trusted by the cloud DRM service.

The **browser** can be cross-platform if the interface to the platform DRM is open.

The portion of the **CDM** in the browser cannot be trusted. The real CDM should be in the TEE.

The **DRM** must be trusted and run in the TEE. As a result, **ECP requirements** segregate the HTML/JS app and browser from the DRM – enabling the app to be more portable.



Fraunhofer FOKUS

DRM Standards – Mapping EME robustness levels to security levels

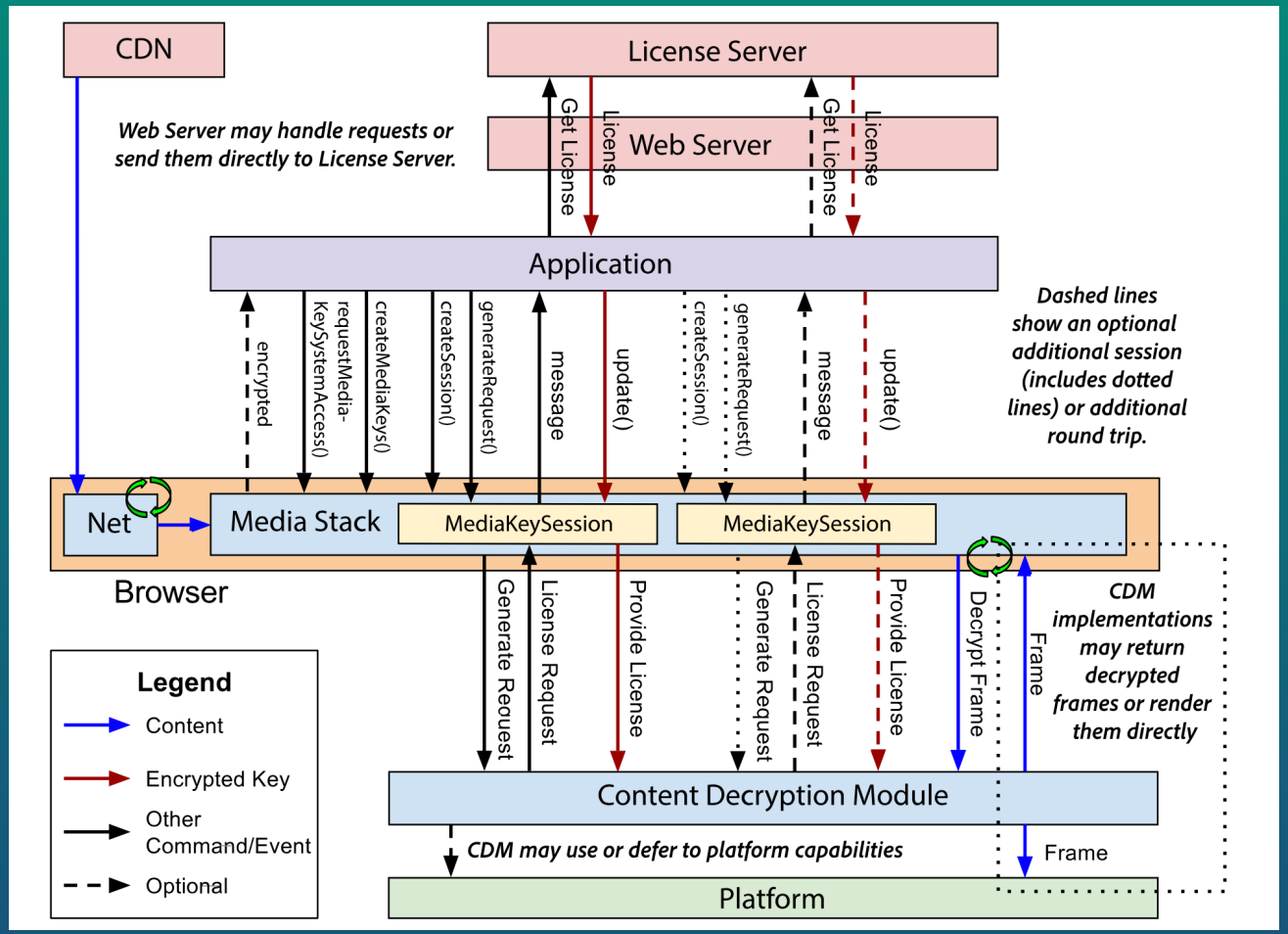
W3C EME Level	PlayReady	FairPlay	Widevine
1	SL2000	(Apple)Baseline	SW_SECURE_CRYPTO (L3)
2	SL2000	(Apple)Baseline	SW_SECURE_DECODE (L3)
3	SL2000	(Apple)Baseline	HW_SECURE_CRYPTO (L2)
4	SL2000	(Apple)Baseline	HW_SECURE_DECODE (L1)
5	SL3000	(Apple)Main	HW_SECURE_ALL (L1)

Fraunhofer FOKUS

DRM Standards – W3C Encrypted Media Extensions

Current version: Recommendation 18 September 2017

- Provides browser APIs to **control playback of encrypted content**
- License/key exchange is controlled by the application
- Does not define a real content protection or Digital Rights Management System
  - Clear Key available in EME browser implementations for baseline level functionality
- Defines API that can be used to discover, select and interact with DRM systems



Source: https://www.w3.org/TR/encrypted-media/

Fraunhofer FOKUS

DRM Standards – What is Clear Key?

- W3C mandates support for Clear Key in EME browser implementations for baseline level functionality
- Should not be used together with real DRM systems
- More secure than only transport (TLS) and/or token authentication when used together
- Plain-text clear (unencrypted) AES keys in JSON Web Key (JWK) format:

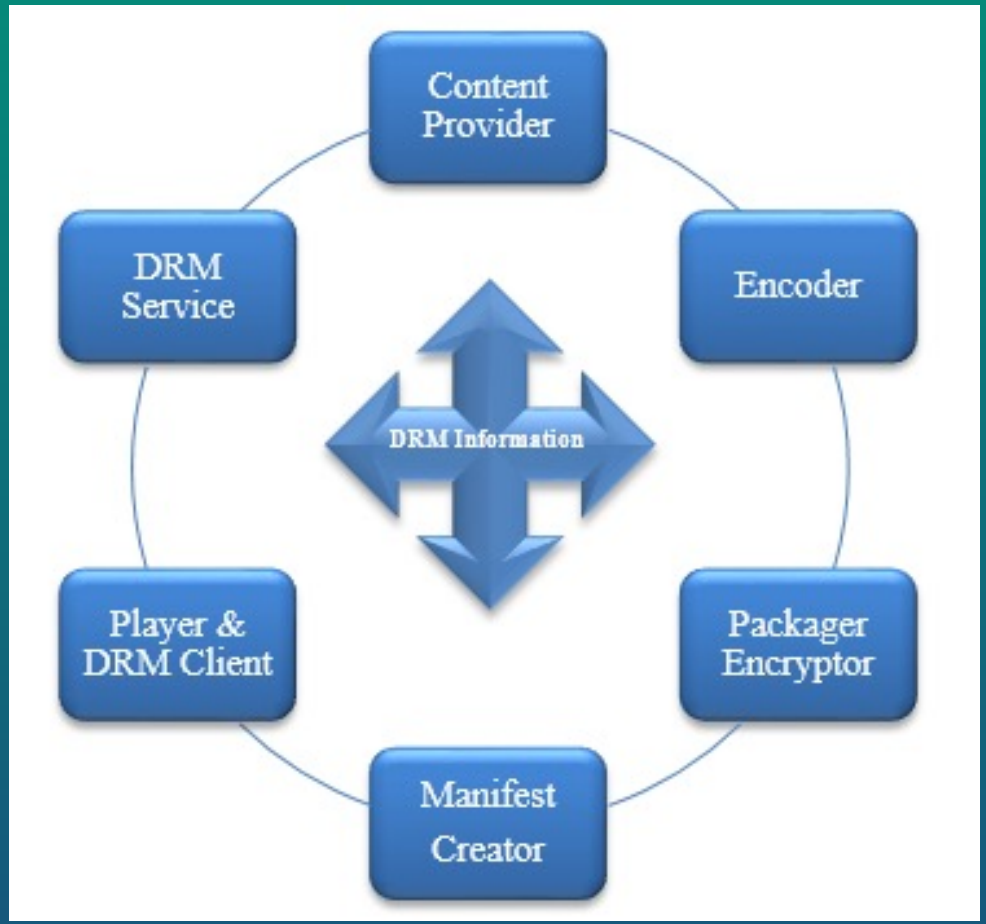
```
{
  "keys":
    [{
      "kty":"oct",
       "k":"tQ0bJVWb6b0KPL6KtZIy_A",
       ”kid":"LwVHf8JLtPrv2GUXFW2v_A"
    }],
   'type':"temporary"
}
```


Fraunhofer FOKUS

DRM Standards - CPIX

- “Content Protection Information Exchange Format” was initially specified by DASH-IF in 2015, currently in version 2.3
  - AWS Secure Packager and Encoder Key Exchange (SPEKE)
  - Also published as ETSI TS 103 799

- CPIX enables key exchange interoperability in multi-DRM environments
  - A CPIX document contains keys and DRM information to be shared among entities in DASH/HLS preparation workflows, e.g., Packager, Encryptor, Manifest creator, DRM service
  - A Player is typically not involved in CPIX exchanges
  - The CPIX document itself can be encrypted, signed and authenticated

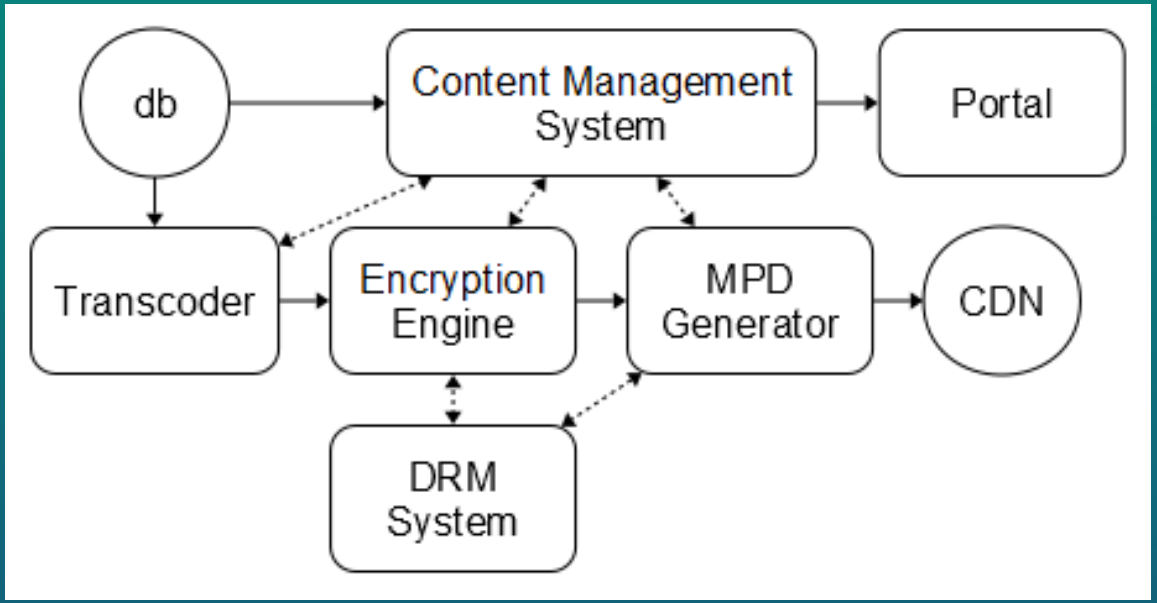


Source: https://dashif.org/docs/CPIX2.3/Cpix.html

Fraunhofer FOKUS

DRM Standards - CPIX – Example Workflow for On-Demand Content

- **CMS** initiates a DASH content preparation
- **Transcoder** receives the unencrypted files and outputs segmented files
- **Encryption Engine** either generates the Content Keys or requests them from the DRM system
- **DRM System** provides information for PSSH boxes and ContentProtection elements in the MPD to the **MPD Generator**
- **DASH content** is uploaded to the CDN
- **The Portal** receives editorial metadata and user access information



Source: https://dashif.org/docs/CPIX2.3/Cpix.html

Fraunhofer FOKUS

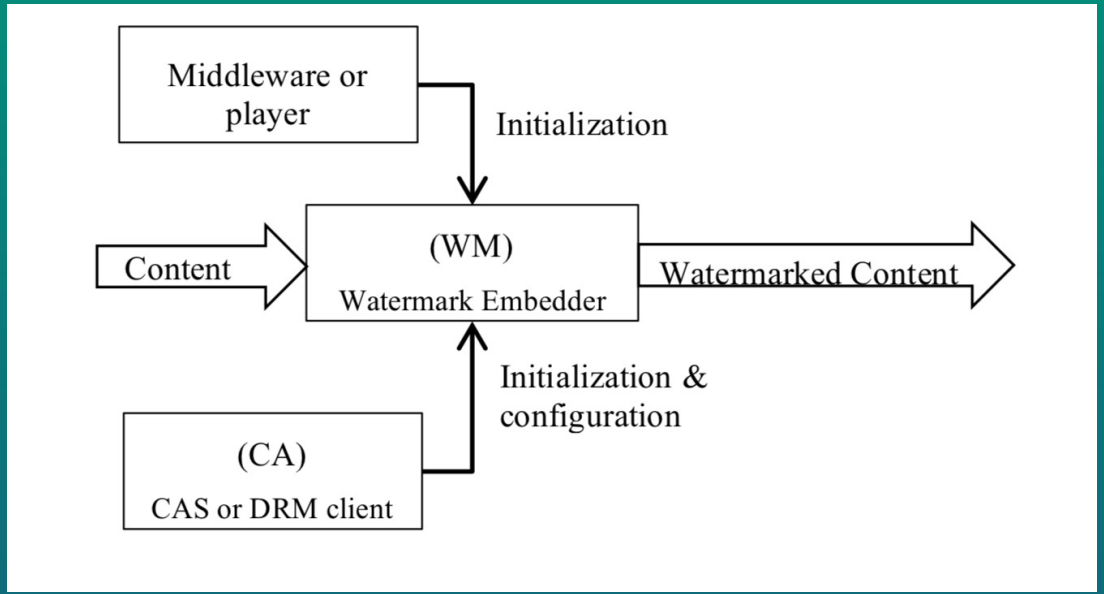
Watermarking

Fraunhofer FOKUS

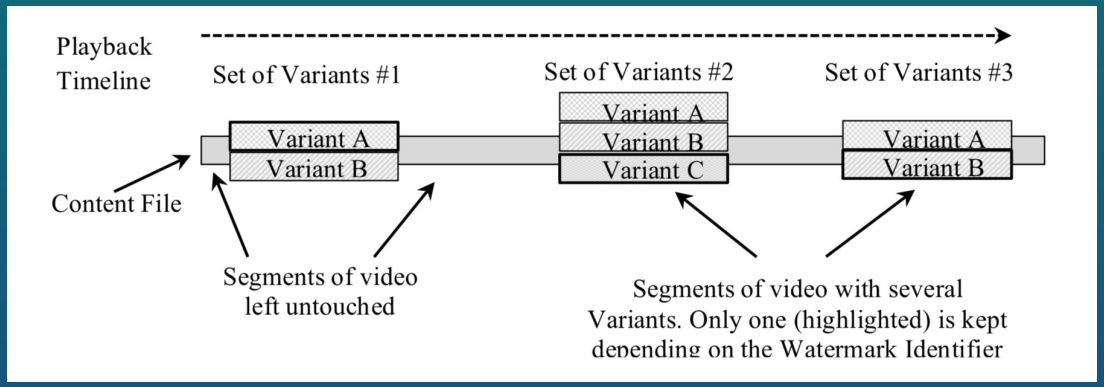
Watermarking – OTT Standardization

UHD Forum Guidelines on Forensic Watermarking

- **One-Step Watermarking**
  During encode on the server OR during playback in the secure video pipeline, e.g. via DRM



- **Two-Step (A/B) Watermarking**
  1. Preprocessing: computes Sets of Variants. Pre-encoder or in compressed domain
  2. watermark embedding: checks Variant Sequence in transit (e.g. network edge) or in the client device (e.g. during playback)

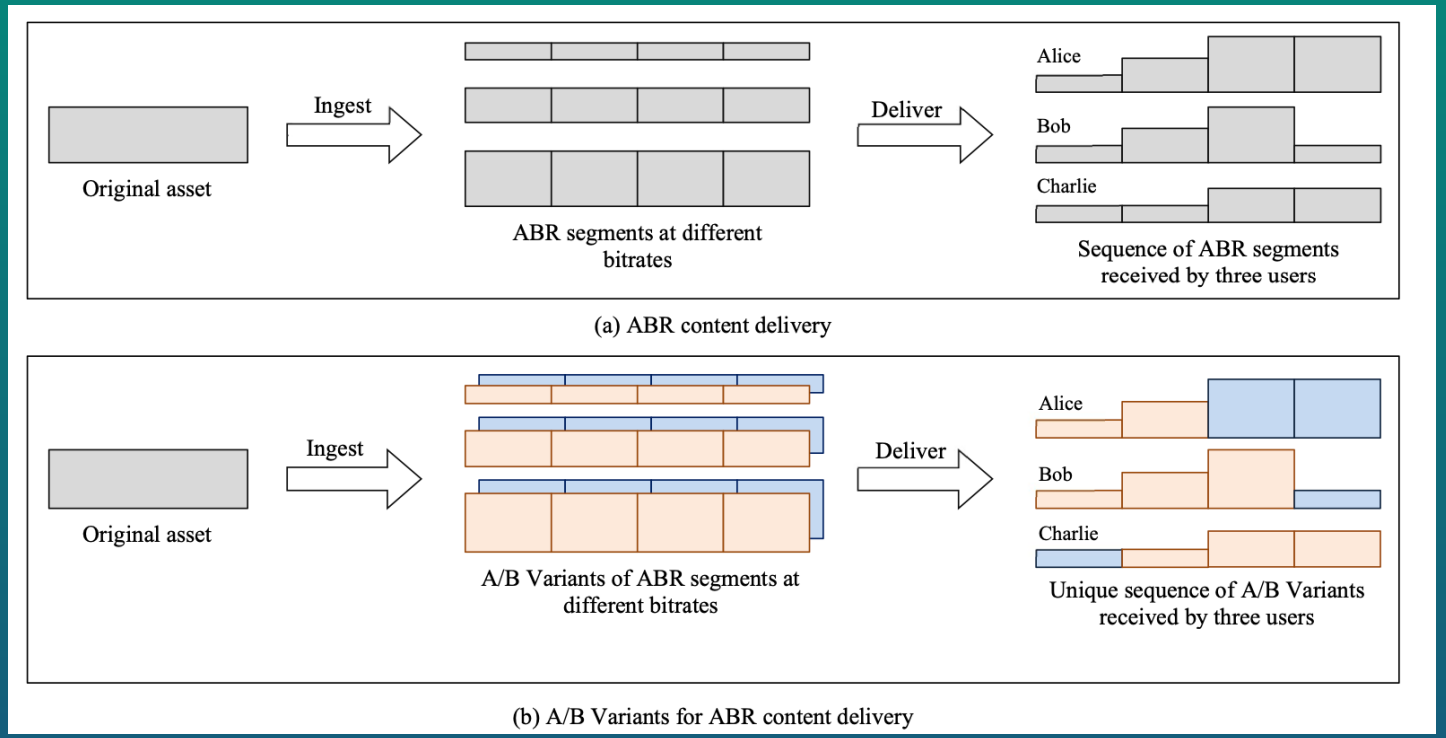


Source: https://ultrahdforum.org/wp-content/uploads/Ultra-HD-Forum-Guidelines-v1.4-final-for-release.pdf

Fraunhofer FOKUS

Watermarking – DASH-IF

- DASH-IF IOP Watermarking specification in community review
- Server-side forensic watermarking using A and B variants of segments (A/B Watermarking)
- Standardized WM token contains the order of A/B Variants and is carried from Transcoder/Watermarker, to Packager, CDN Origin and CDN Edge
- Streaming format agnostic -> Compatible with DASH & HLS



Fraunhofer FOKUS

Cross-platform Streaming

Fraunhofer FOKUS

Cross-platform Streaming - CMAF + DRM support

Streaming	File Format	CENC mode	DRM
DASH	ISOBMFF (CMAF)	‘cenc’	PlayReady PK<4.0, Widevine
DASH	ISOBMFF (CMAF)	‘cbcs’	PlayReady PK>4.0, >Android N, Chromecast

Streaming	File Format	CENC mode	DRM
HLS	MPEG2TS	AES-128 / Sample-AES	FairPlay
HLS	ISOBMFF (CMAF)	Sample-AES ‘cbcs’	FairPlay

→With CMAF segments, HLS and DASH manifests can reference the same file format

→‘cenc’ is needed for legacy devices.

→‘cbcs’ for modern devices

Cross-platform Streaming - What can your browser do?

Simple check on MSE and EME support

using **MediaSource.isTypeSupported** and

navigator.requestMediaKeySystemAccess

functions.

https://research.akamaized.net/capabilitiescheck.html

Decryption skills...

System	Encryption	Robustness	Supported?
Widevine	cenc	L3 - SW crypto	yes
Widevine	cenc	L2 - HW crypto	no
Widevine	cenc	L1 - HW all	no
Widevine	cbcs	L3 - SW crypto	yes
PlayReady	cenc		no
PlayReady	cbcs		no
ClearKey	cenc		yes
ClearKey	cbcs		yes
Fairplay	cbcs		no

Decoding skills....

Codec	String	Supported?
H.264 Baseline 1.3	avc1.42000d	yes
H.264 Main 3.0	avc1.4d001f	yes
H.264 High 4.0	avc1.640028	yes
H.264 High 5.2	avc1.640034	yes
HEVC MP MT 3.1	hev1.1.6.L93.B0	no
HEVC Dolby Vision 5.6	dvh1.05.06	no
VP9 P0 L5 8b	vp09.00.50.08	yes
AV1 MP L2.0 MT 8b	av01.0.00M.08	yes
AAC-LC	mp4a.40.2	yes
Dolby Digital	ec-3	no

Cross-platform Streaming - Types of browser-based playback

Type 1

- Direct playback via the HTML5 video element: *<video id="video" controls width=1280 height=720 src="video.mpd"></video>*
- No control over the playback and the ABR behavior of the player
- Examples: HbbTV, Samsung AVPlay, Safari HLS

Type 2

- HTML5 video element but ABR API to control ABR logic of the player
- Examples: Smart TV APIs

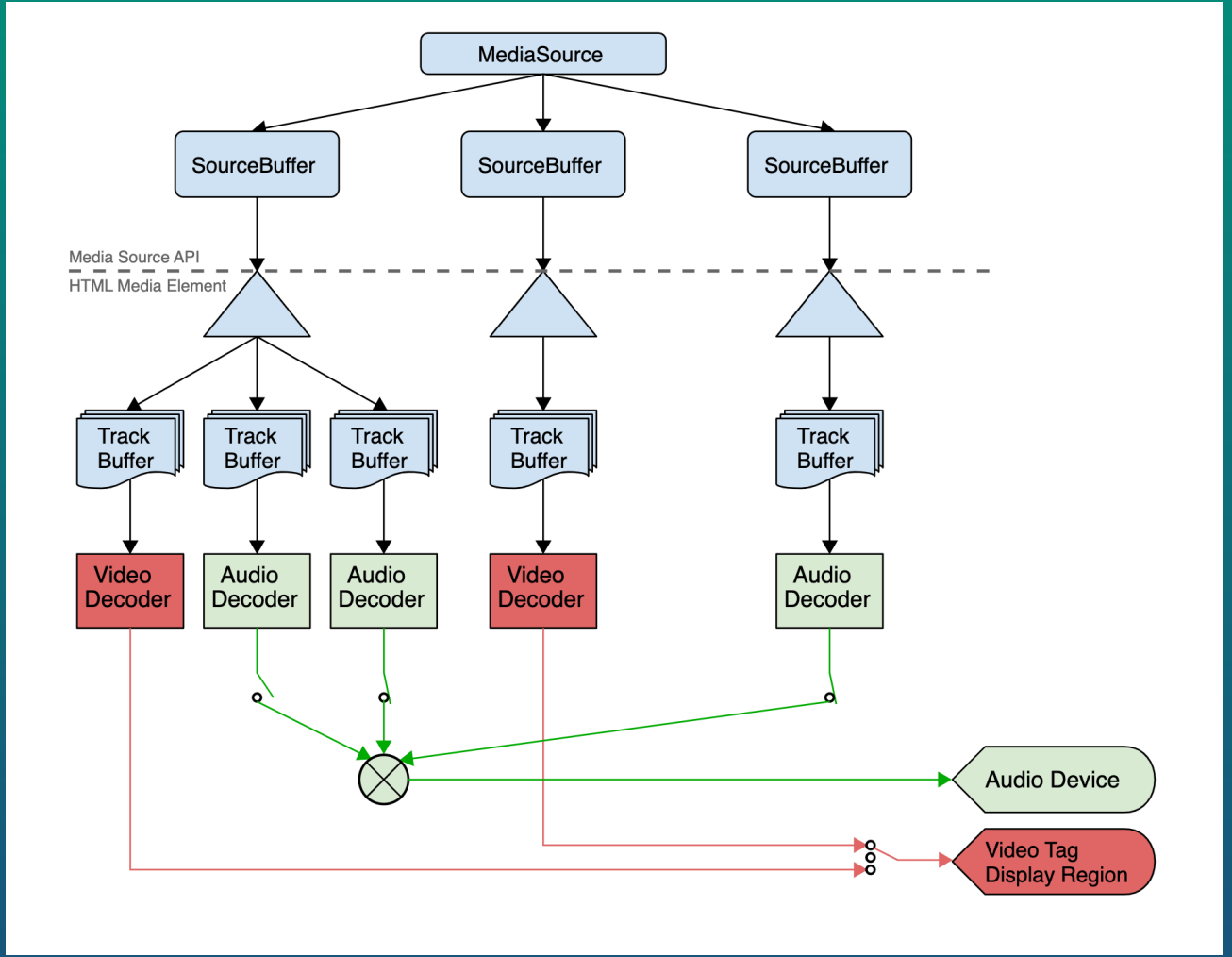
Type 3

- HTML5 video element + Media Source Extensions (MSE) + Encrypted Media Extensions (EME)
- Full control over the playback but player logic needs to be implemented
- Examples: dash.js, hls.js, Shaka Player

Fraunhofer FOKUS

Cross-platform Streaming – W3C Media Source Extensions

- Enables JavaScript clients to append media segments to the HTML5 Video Element
- Defines a **MediaSource** object that can serve as a source of media data for an HTMLMediaElement.
- MediaSource objects have one or more **SourceBuffer** objects
- Applications append data segments to the SourceBuffer objects, and can adapt the quality of appended data based on system performance and other factors
- Proposal: **ManagedMediaSource API**
  - enabled on **Safari 17 beta** on macOS and iPadOS and behind an experimental flag on **iOS** for now.
  - More details: Low memory availability/notification, network streaming changes, quality selection



Fraunhofer FOKUS

Cross-platform Streaming – Player Overview

dash.js	Web Browser	Chrome
		Firefox
		Edge
	TV	Samsung
		LG
		Chromecast
HTML Type 1	Safari	iOS
		iPadOS
	TV	Samsung
		LG
	STB	
ExoPlayer	Android Mobile	
	Android TV	FireTV
		Sony
		Philips
AVFoundation	iOS	
	iPadOS	
	tvOS	

Cross-platform Streaming - Overview

			Video Codecs				AES scheme		DRM/Max Security Level		
Device	OS	Version	AVC	HEVC	VP9	AV1	cbcs	cenc	Widevine	PlayReady	FairPlay
Chrome	Win/MacOS	>=104	YES	YES	YES	YES	YES	YES	YES/L3		
Chrome	Win	>=104	YES	YES	YES	YES	YES	YES	(YES/L1)		
Safari	MacOS	>=11	YES	YES	YES		YES				YES
Firefox	Win/MacOS	>=60	YES		YES	YES	YES	YES	YES/L3		
Edge (Chromium)	Win	88	YES	YES	YES	(YES)	YES	YES	YES/L3	(YES/SL3000)	
iPhone/AppleTV	iOS/tvOS	>=10	YES	YES	YES		YES				YES
Safari	iOS/ipadOS	>=10	YES	YES			YES				YES
Chrome	Android	>=7.1	YES		YES		YES	YES	YES/L2		
Mobile	Android	>=7.1	YES	YES	YES		YES	YES	YES/L1		
Sony/Philips	Android TV	>=2021	YES	YES	YES	YES	YES	YES	YES/L1	YES	
Magenta TV Stick	Android TV	10	YES	YES	YES		YES	YES	YES/L1	YES	
Fire TV	FireOS	>=7	YES	YES	YES	(YES)	YES	YES	YES/L1	YES/SL3000	
Samsung	Tizen	>=5.5 (2020)	YES	YES	YES	YES	YES	YES	YES/L1	YES/SL3000	
LG	WebOS TV	>=5.0 (2020	YES	YES	YES	YES	YES	YES	YES/L1	YES/SL3000	
Chromecast Ultra / G	Android TV		YES	YES	YES		YES	YES	YES/L1	YES/SL2000	
Roku	Roku OS	>=9.0	YES	YES	YES		YES	YES	YES/L1	YES/SL3000	

Source: https://websites.fraunhofer.de/video-dev/is-this-the-end-of-cenc-an-overview-of-drm-codec-support-in-2021/

Fraunhofer FOKUS

Streaming Analytics

Fraunhofer FOKUS

Motivation for Streaming Analytics

Viewers start abandon streams that take more than 2 seconds to startup

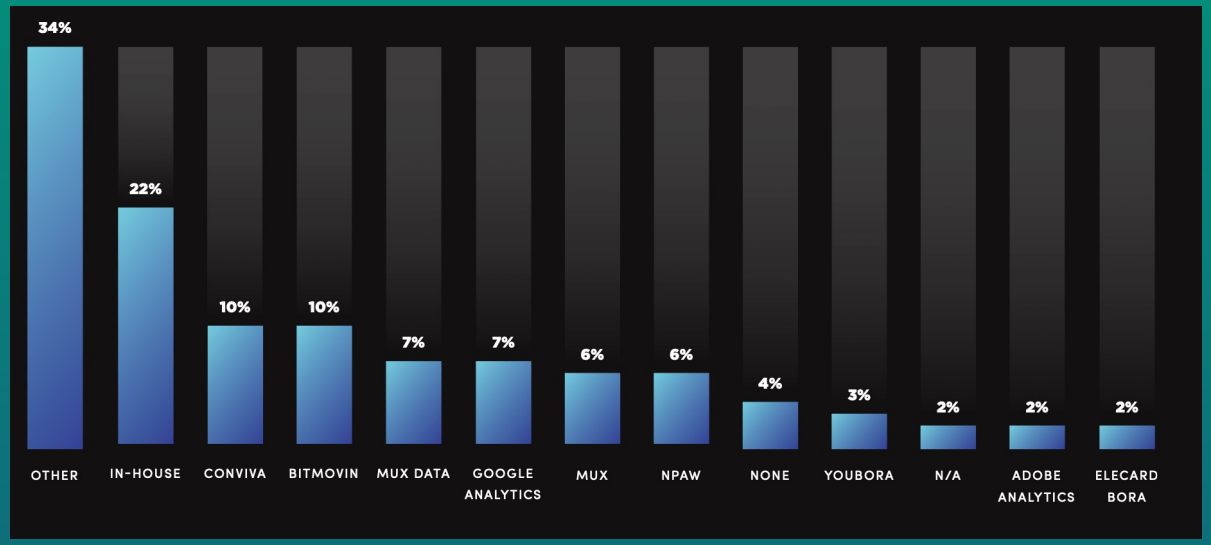
1% of rebuffering causes people to watch 5% less of a video

Viewers who experience video failure are less likely to revisit a web page

40% of customers are unlikely to give a streaming service a chance on a second device after being confronted with an inferior stream

Source: “Video Stream Quality Impacts Viewer Behavior: Inferring Causality Using Quasi-Experimental Designs”, IEEE/ACM Transactions on Networking, Krishnan and Sitaraman, Akamai

Streaming Analytics Solutions



- Streaming Analytics Standards:
  - SAND
  - CMCD
  - CTA-2066
- Goals
  - Improve interoperability
  - Better comparison
  - Common language

Source: Source: Bitmovin Video Developer Report 2022-2023

Fraunhofer FOKUS

CMCD – Common Media Client Data

- Published as CTA-5004 in September 2020 out of CTA WAVE group
- Media player clients can convey information to Content Delivery Networks (CDNs) with each object request
  - ✓ useful in log analysis, QoS monitoring and delivery optimization
  - ✓ improve the quality of service offered by CDNs
- Transport via
  - ✓ custom HTTP request header,
  - ✓ HTTP query argument,
  - ✓ As a JSON object independent of the HTTP object request
- Integrated with dash.js -> see Blog Post

CMCD parameters

- bl: Buffer length
- br: Encoded bitrate
- bs: Buffer starvation
- cid: Content ID
- d: Object duration
- dl: Deadline
- mtp: Measured throughput
- nor: Next object request
- nrr: Next range request
- ot: Object type
- pr: Playback rate
- rtp: Requested maximum throughput
- sf: Streaming format
- sid: Session ID
- st: Stream Type
- su: Startup
- tb: top bitrate

Fraunhofer FOKUS

CMSD – Common Media Server Data

- Published as CTA-5006 in November 2022
- uniform method for media servers to exchange data with each media object response
- The aim is to enhance distribution efficiency, performance, and ultimately, the user experience

Open source Implementations:

- added to dash.js
- Origin implementations from Unified Streaming and National University of Singapore/Ozyegin University

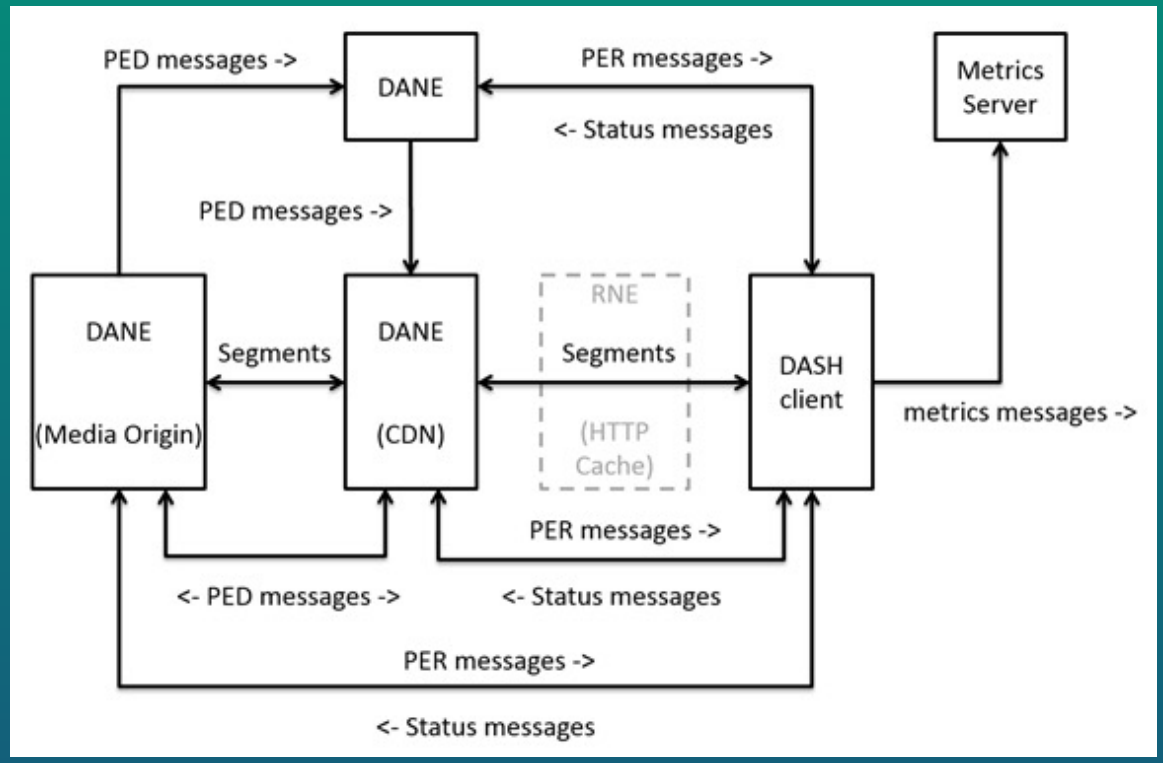
CMSD parameters

- at: Availability Time
- du: Duress
- br: Encoded bitrate
- etp: Estimated throughput
- ht: Held time
- n: Intermediary identifier
- mb: Max suggested bitrate
- nor: Next object response
- nrr: Next range response
- d: Object duration
- ot: Object type
- rd: Response delay
- rtt: Round trip time
- su: Startup
- st: Stream Type
- sf: Streaming format
- v: Version

Fraunhofer FOKUS

SAND

- Published as ISO/IEC 23009-5:2017 Server and network assisted DASH (SAND)
- Introduces bi-directional messages between DASH clients and network elements or between various network elements for the purpose to improve efficiency of streaming sessions
- Standardized metric categories (23009-1 Annex D):
  - TCPList, HTTPList, RepSwitchList, BufferLevel, PlayList, DeviceInformationList
- Example Use Cases:
  - Metric reporting
  - Shared Resource Allocation
  - Real-time Multi-CDN switching
  - And many more …see DASH-IF whitepaper: https://dashif.org/docs/SAND-Whitepaper-Dec13-final.pdf



Fraunhofer FOKUS

SAND Shared Ressource Allocation

Use cases:

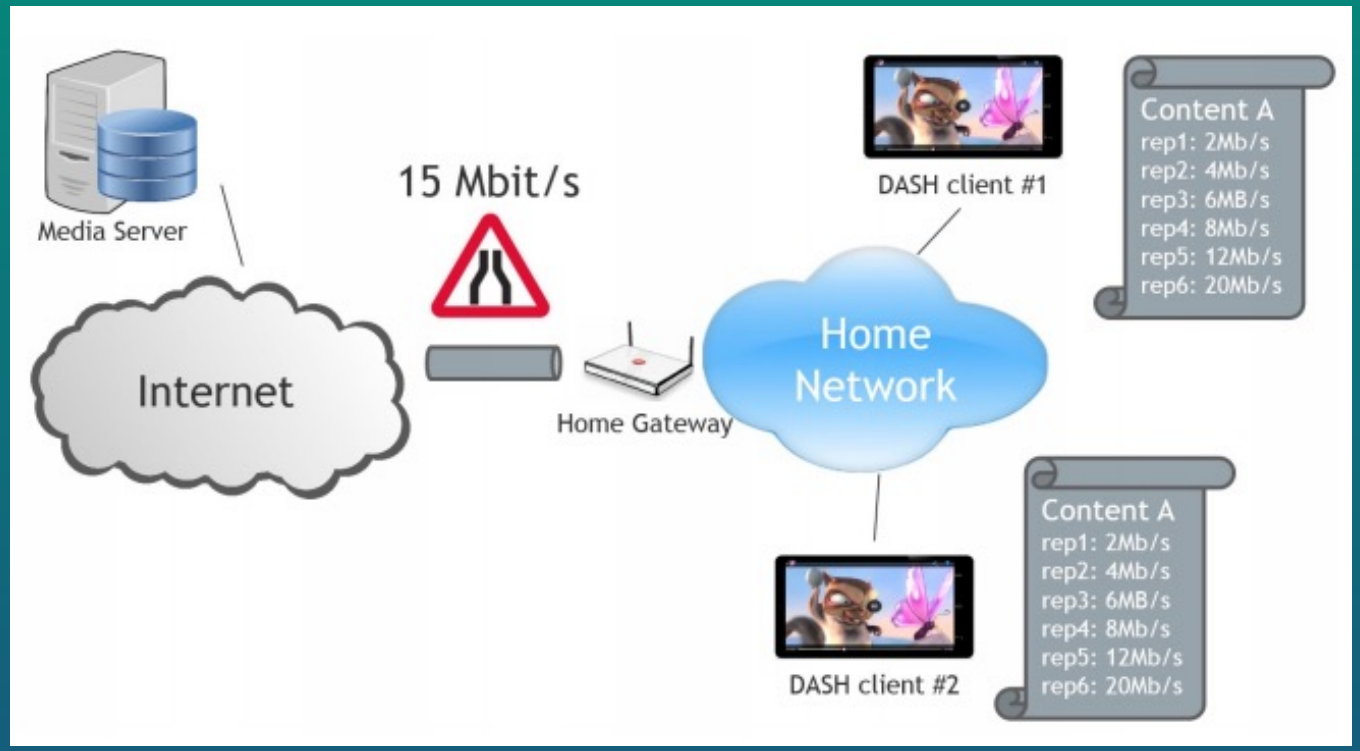
- Sports events (stadium)
- Airplanes, trains
- Home networks

Goal:

- Controlling the available bandwidth
- Use bandwidth optimally

Different Strategies

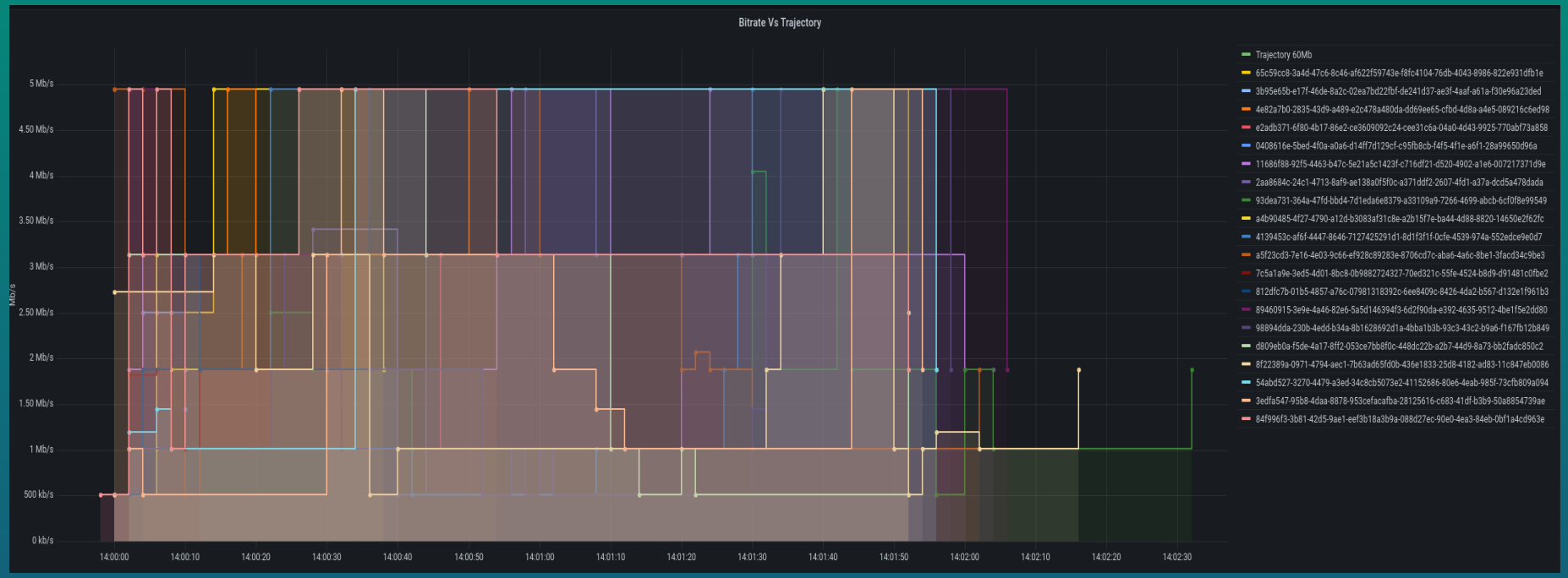
- „Everybody served“
- “Premium privileged“
- Etc.



Fraunhofer FOKUS

Challenge: Multiple Clients – Shared Network Bottleneck

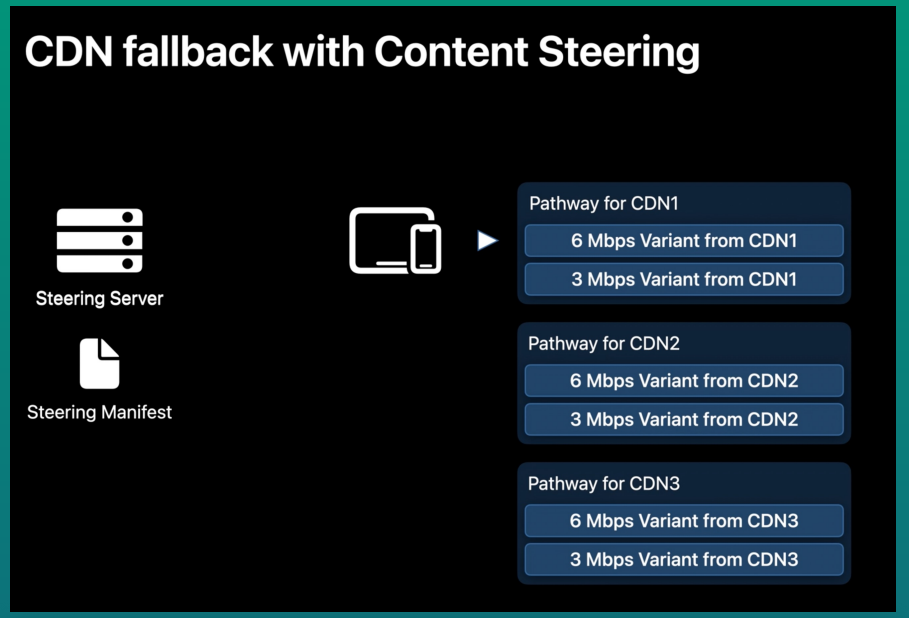
- ABR clients not aware of each other → aggressiveness
- Oscillating ABR behavior when connected to the same network bottleneck
- Increasing bandwidth requirements (UHD, HDR etc. etc.)
- Bandwidth limited and underutilized

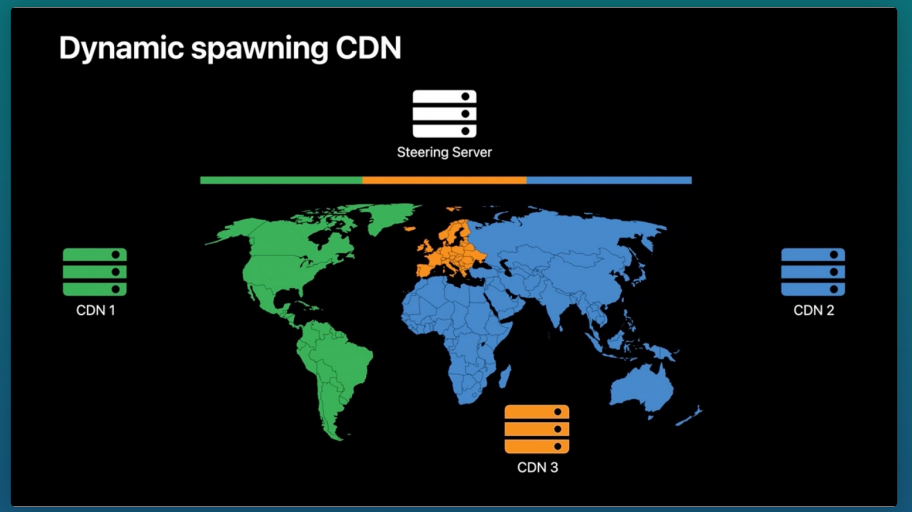


Fraunhofer FOKUS

HLS Content Steering

- Introduced at WWDC21
- Groups redundant variants into Pathways
- Steering Server provides **Steering Manifest (JSON)** to clients for Load Balancing (e.g. order of CDNs)
- New **Pathway** cloning to **dynamically add CDNs** to existing clients





Fraunhofer FOKUS

HLS Content Steering

New playlist syntax

```
#EXTM3U
#EXT-X-CONTENT-STEERING:SERVER-URI="/steering?video=00012",PATHWAY-ID="CN"

#EXT-X-STREAM-INF:BANDWIDTH=1280000,CODECS="avc1.640028",PATHWAY-ID="CN"
https://cn.example.com/low/audio-video.m3u8
#EXT-X-STREAM-INF:BANDWIDTH=7680000,CODECS="avc1.640028",PATHWAY-ID="CN"
https://cn.example.com/hi/audio-video.m3u8

#EXT-X-STREAM-INF:BANDWIDTH=1280000,CODECS="avc1.640028",PATHWAY-ID="JP"
https://jp.example.com/low/audio-video.m3u8
#EXT-X-STREAM-INF:BANDWIDTH=7680000,CODECS="avc1.640028",PATHWAY-ID="JP"
https://jp.example.com/hi/audio-video.m3u8

#EXT-X-STREAM-INF:BANDWIDTH=1280000,CODECS="avc1.640028",PATHWAY-ID="SG"
https://sg.example.com/low/audio-video.m3u8
#EXT-X-STREAM-INF:BANDWIDTH=7680000,CODECS="avc1.640028",PATHWAY-ID="SG"
https://sg.example.com/hi/audio-video.m3u8
```

HLS Manifest with Content Steering details

- Multiple equal streams on multiple CDNs

Steering Manifest response

```
{
  "VERSION": 1,
  "TTL": 300,
  "PATHWAY-PRIORITY": [ "CN", "JP", "SG" ]
}
```

Steering Manifest includes:

- Priority list of CDN Ids
- Reload time in seconds (TTL) for client to fetch Steering Manifest again

Fraunhofer FOKUS

Content Steering for DASH

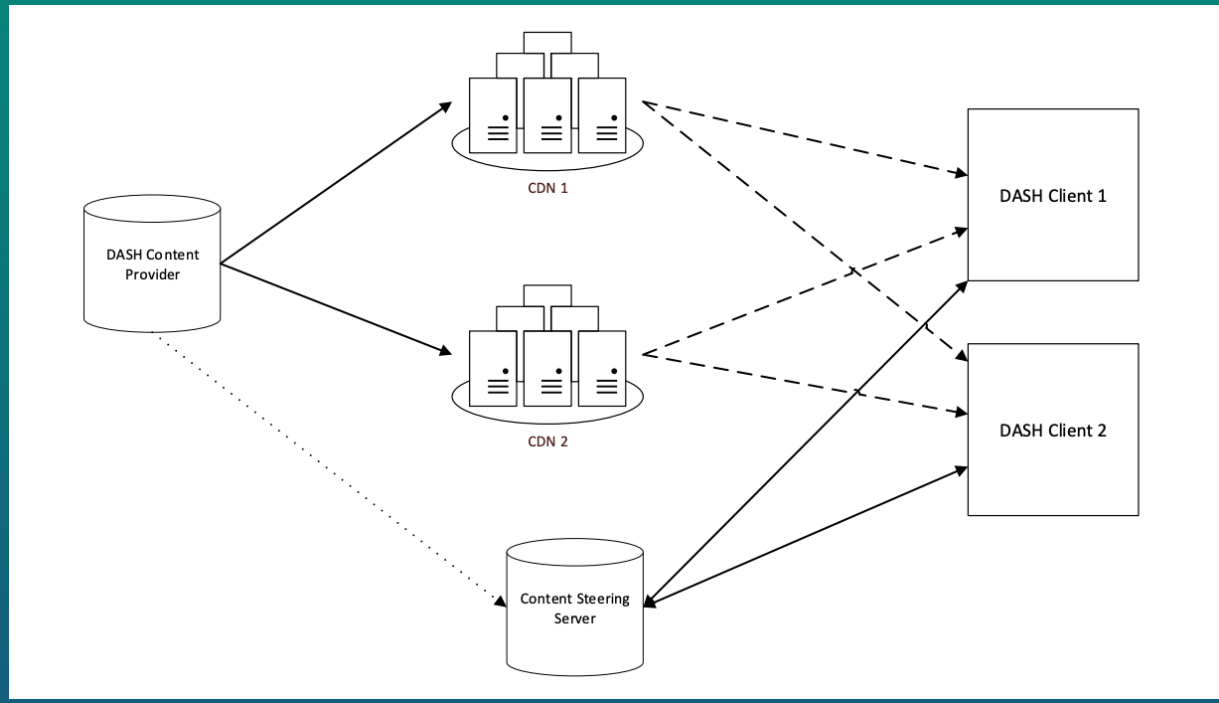
<BaseURL>

```
<BaseURL
serviceLocation="alpha">https://cdn1.example.com/</BaseURL>

<BaseURL
serviceLocation="beta">https://cdn2.example.com/</BaseURL>
```

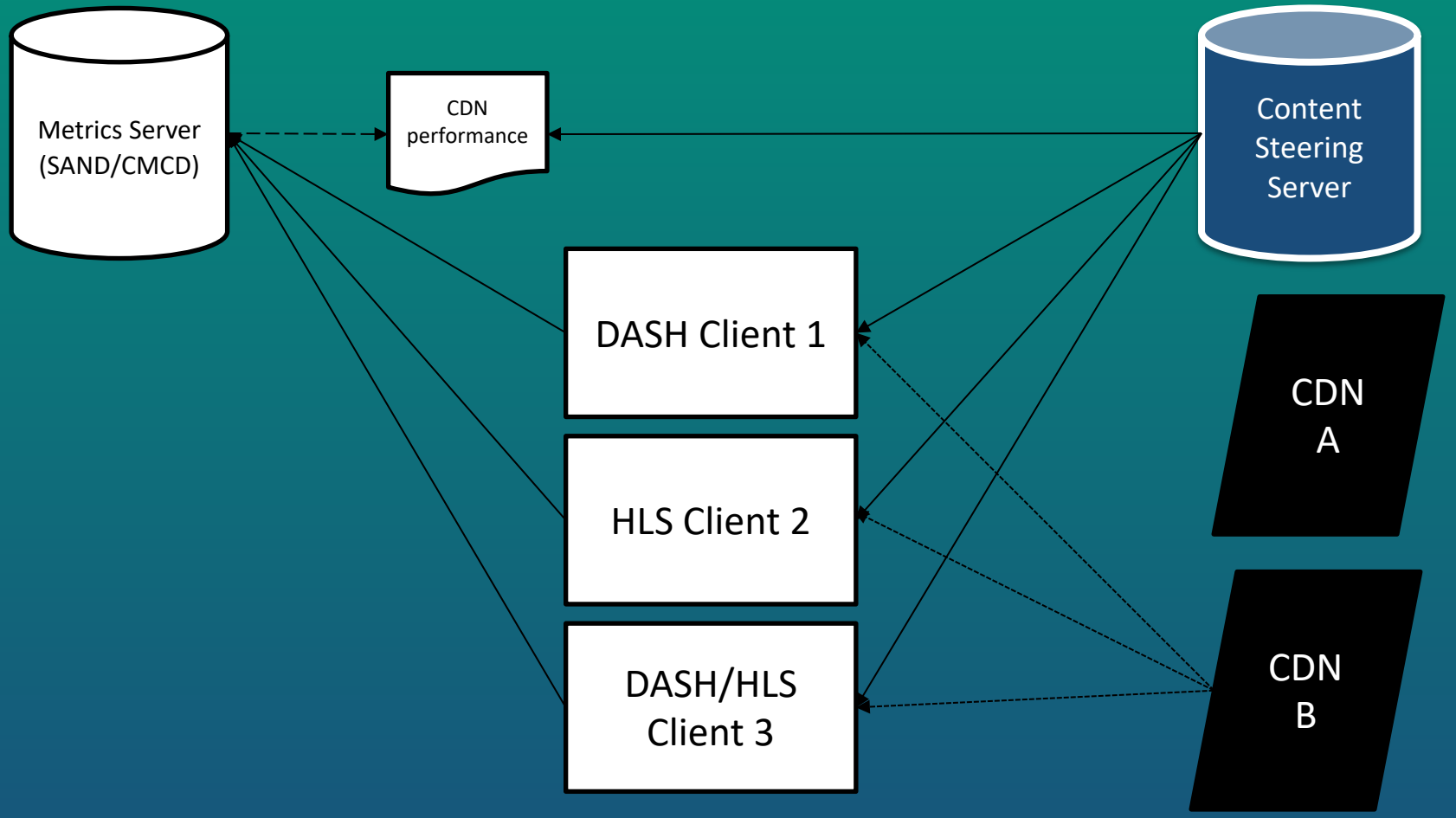
<ContentSteering>

```
<ContentSteering defaultServiceLocation="beta"
queryBeforeStart="true"> https://steeringserver.com/json
</ContentSteering>
```



Fraunhofer FOKUS

Content Steering Demo



Fraunhofer FOKUS

Vielen Dank für Ihre Aufmerksamkeit

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS

Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
info@fokus.fraunhofer.de
www.fokus.fraunhofer.de

Stefan Pham
Tel. +49 (30) 34 63 - 7103
stefan.pham@fokus.fraunhofer.de

Fraunhofer FOKUS