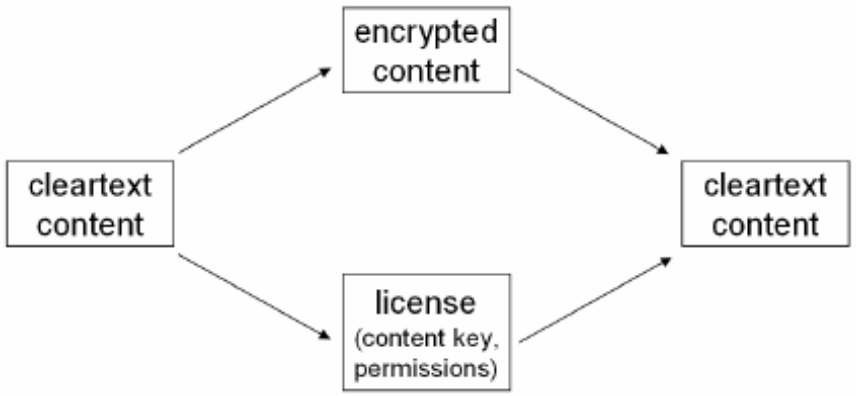
DRM PROTECTED DYNAMIC ADAPTIVE HTTP STREAMING

FRANK HARTUNG, SINAN KESICI, DANIEL CATREIN
ERICSSON RESEARCH, AACHEN, GERMANY

Digital Rights Management (DRM)

- Content protection remains a necessity for certain business models
  - Movies: phased marketing, cinema → DVD → pay TV → free TV
  - All subscription, pay-per-something, rental business models
  - Eases secure sharing in a domain, and backup
  - Not necessary for simple sell-through

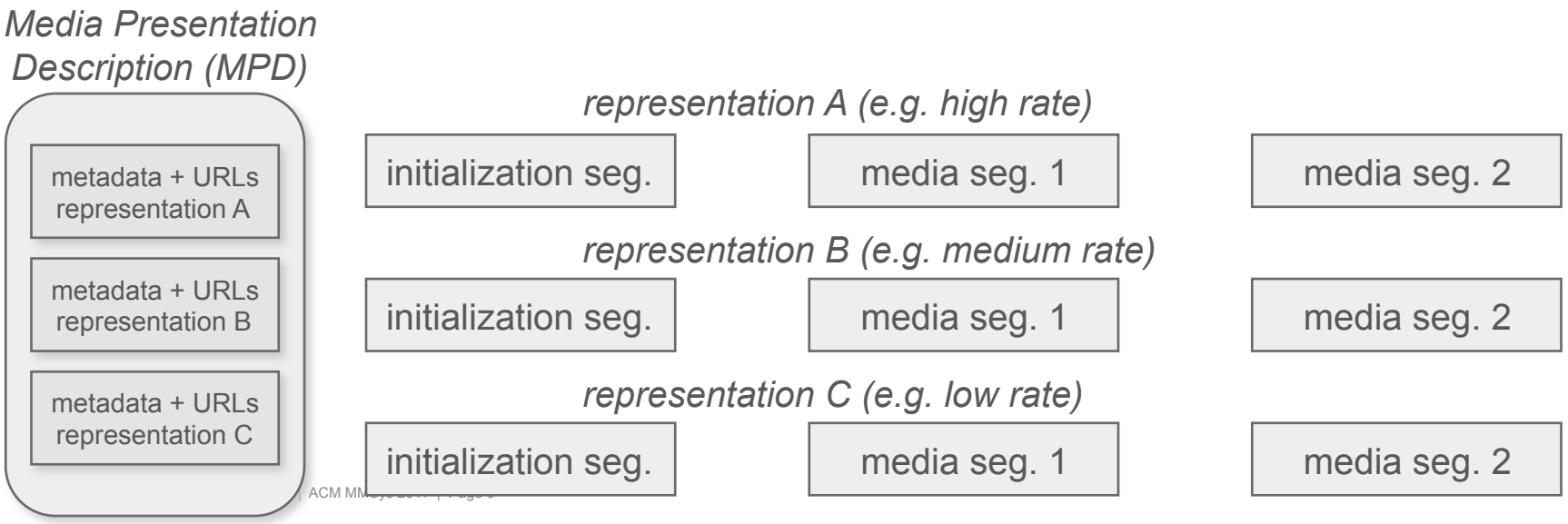
- Basic principle of DRM
  - asset is encrypted
  - a "license" contains the decryption key + policies
  - protection of the license is the hard problem
    - often public-key encryption is used



- Some well-known DRMs: Microsoft Playready, Apple Fairplay, Marlin Broadband, Open Mobile Alliance (OMA) DRM

Dynamic adaptive HTTP streaming (DASH)

- RTP and its variants were previously the preferred streaming protocols
- Now: use of HTTP for concatenated transport of short video segments
  - reliability, congestion fairness, firewall traversal, costs (cloud servers, standard caches)
- Microsoft Smoothstreaming, Apple HLS; 3GPP AHS, OIPF HAS, MPEG DASH

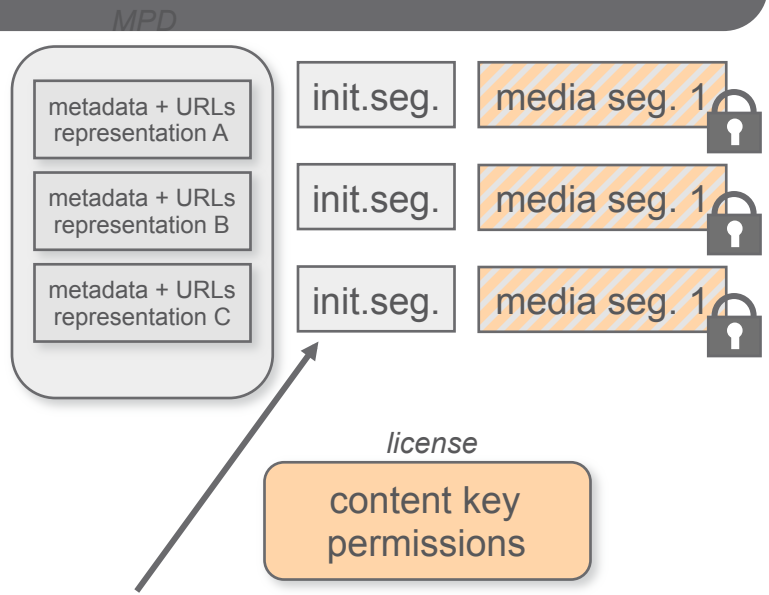


Protection signaling in the MPD (3GPP AHS R9)

MPD				E	1	M	The root element that carries the Media Presentation Description for a Media Presentation.
	Period			E	1…N	M	Provides the information of a Period
		Representation		E	1..N	M	This element contains a description of a Representation.
			ContentProtection	E	0...N	O	This element provides information about the use of content protection for the segments of this representation. When not present the content is not encrypted or DRM protected.
			schemeIdUri	A		M	Provides an URI to identify the content protection scheme. This URI should be an URN or an absolute URL used as an identifier. This attribute, possibly in conjunction with the SchemeInformation element, enables a client to determine compatibility for the content protection technologies required to play the protected segments of this representation, such as the DRM system(s), encryption algorithm(s), and key distribution scheme(s).
				SchemeInformation	E	0,1	O	This element gives the information about the used content protection scheme. The element can be extended in a separate namespace to provide more scheme specific information. For more details refer to section 12.7.1.

DRM use-cases and Requirements

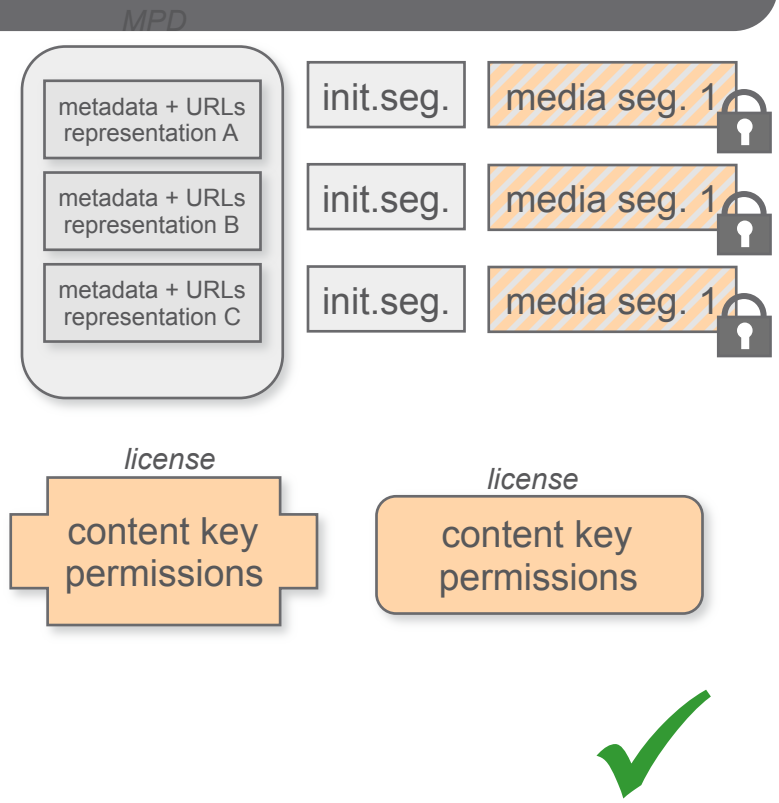
- Basic requirement
  - encryption of DASH segments
  - enable receiving device to check for existence of DRM license
  - enable receiving device to acquire DRM license
  - DRM system agnostic



information necessary to check for existence of license, and for acquiring license

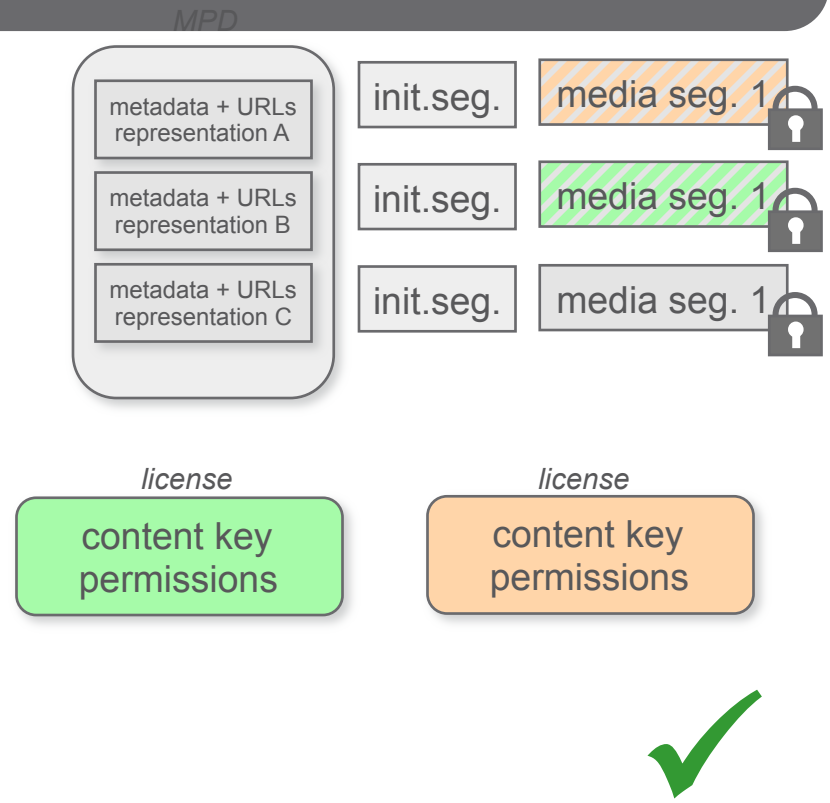
DRM use-cases and Requirements

- Additional requirements
  - allow use of different DRM systems for key management in parallel
  - pay-per-quality
  - bundle video channels into a channel group / “channel bouquet”
    - accessed with one common license
  - pay-per-view (PPV) segments / key change
  - pay-per-maximum-quality



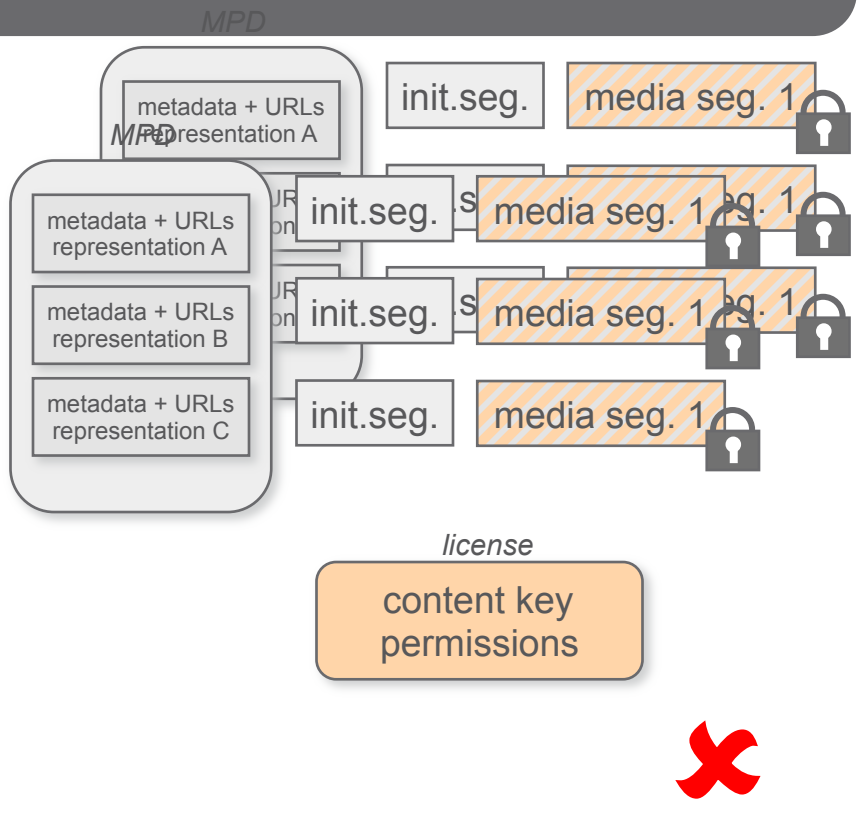
DRM use-cases and Requirements

- Additional requirements
  - allow use of different DRM systems for key management in parallel
  - pay-per-quality
  - bundle video channels into a channel group / “channel bouquet”
    - accessed with one common license
  - pay-per-view (PPV) segments / key change
  - pay-per-maximum-quality



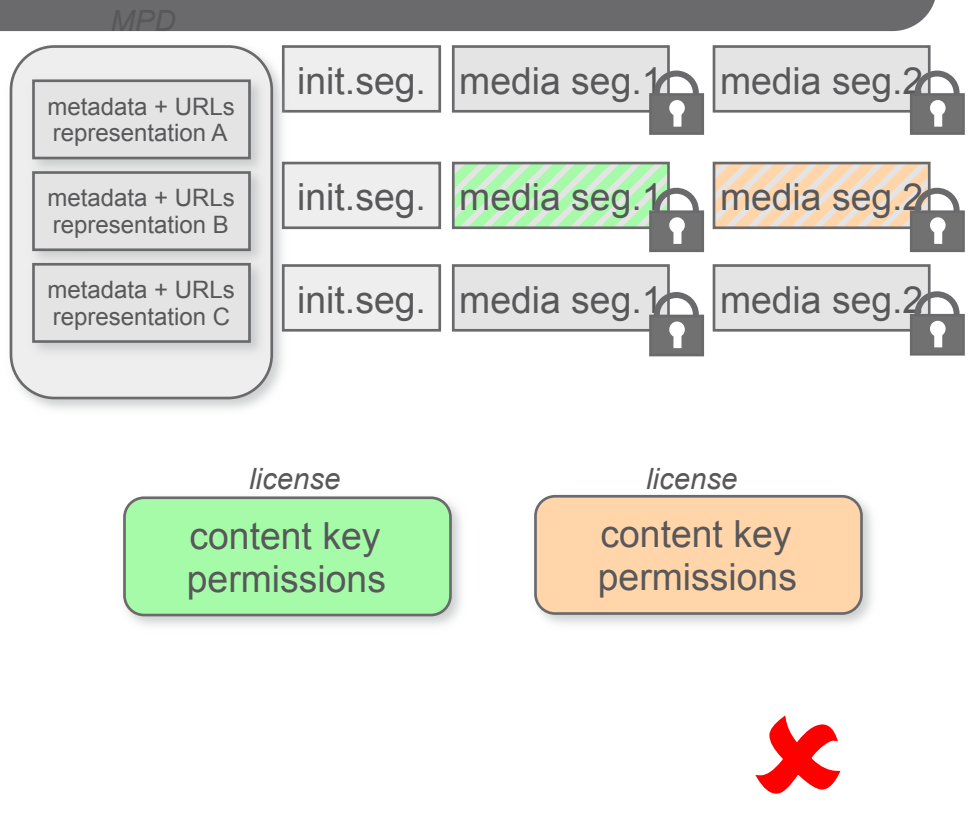
DRM use-cases and Requirements

- Additional requirements
  - allow use of different DRM systems for key management in parallel
  - pay-per-quality
  - bundle video channels into a channel group / “channel bouquet”
    - accessed with one common license
  - pay-per-view (PPV) segments / key change
  - pay-per-maximum-quality



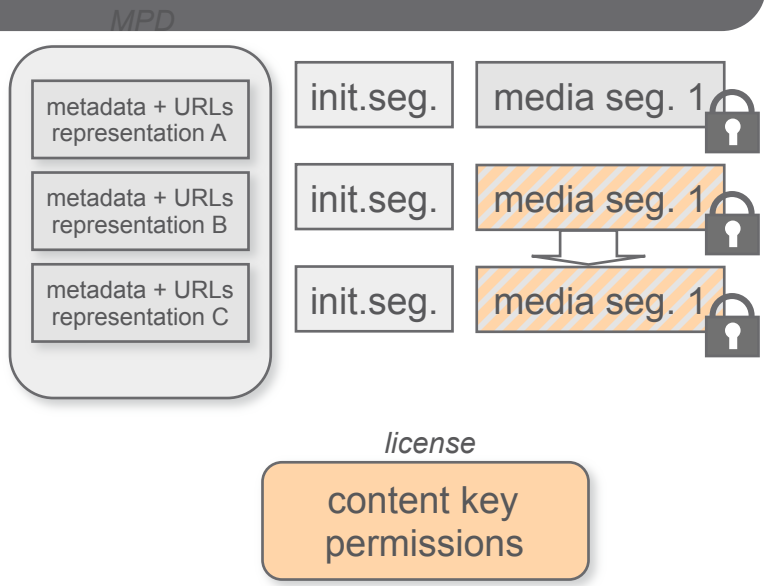
DRM use-cases and Requirements

- Additional requirements
  - allow use of different DRM systems for key management in parallel
  - pay-per-quality
  - bundle video channels into a channel group / “channel bouquet”
    - accessed with one common license
  - pay-per-view (PPV) segments / key change
  - pay-per-maximum-quality



DRM use-cases and Requirements

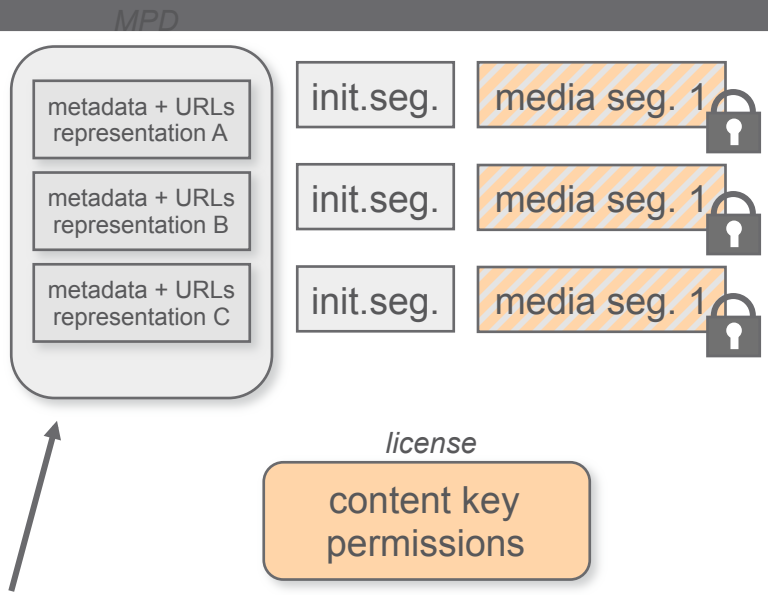
- Additional requirements
  - allow use of different DRM systems for key management in parallel
  - pay-per-quality
  - bundle video channels into a channel group / “channel bouquet”
    - accessed with one common license
  - pay-per-view (PPV) segments / key change
  - pay-per-maximum-quality



Enabling the use cases: 1. more signaling in MPD

- 1. Add more signaling to MPD
  - Content Identifier
  - Rights issuer URL
  - Pay-per-view indicator

→early license acquisition

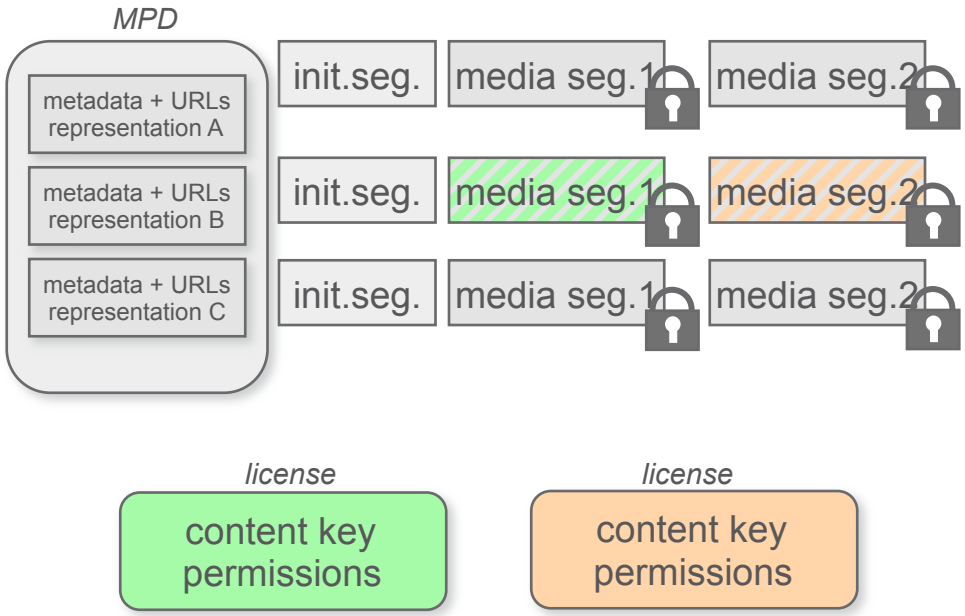


information necessary to check for existence of license, and for acquiring license

Enabling the use cases:
2. protection Signaling per segment

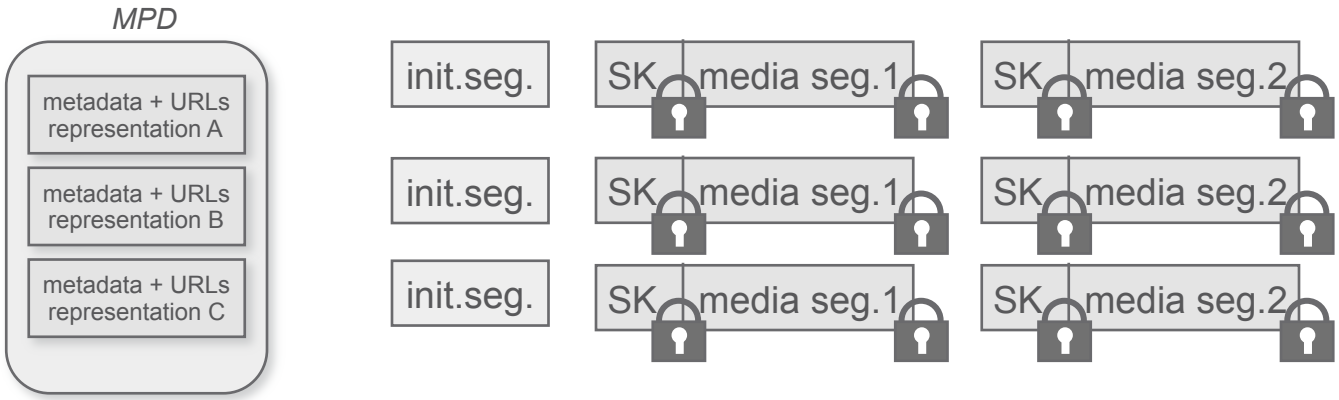
› 2. Signaling per segment instead of per representation

→ key change



Enabling the use cases:
3. Use of Short-term keys

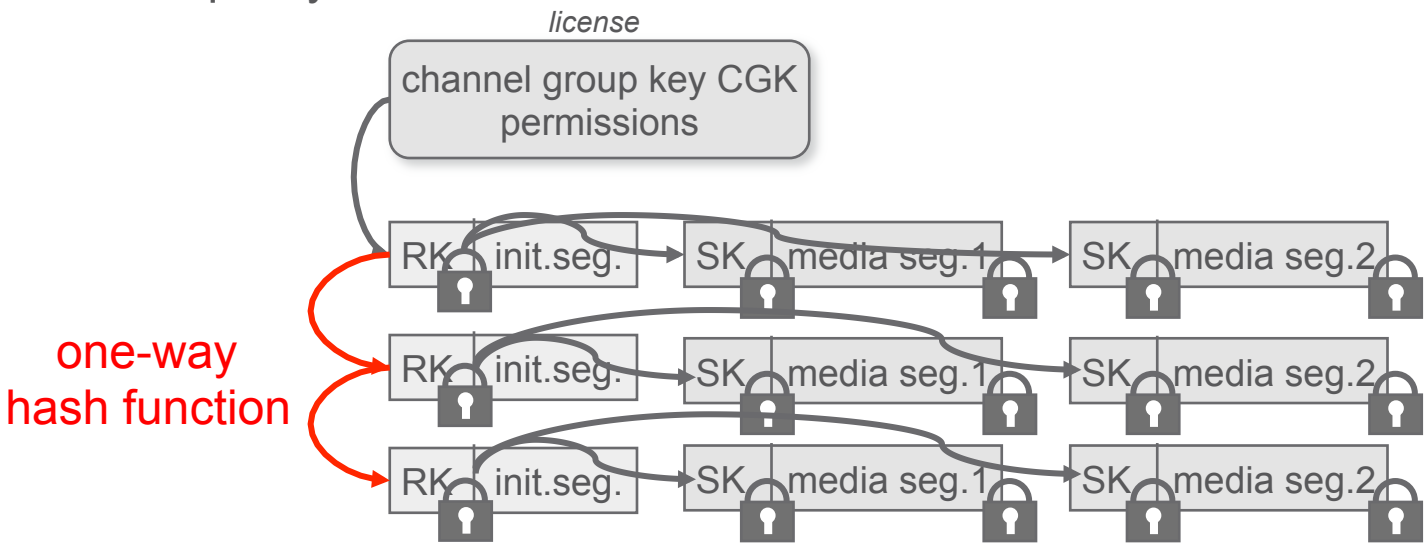
- 3. Use short-term (per segment) keys, transported in the segment (encrypted)
  - each SK is individual for the respective segment



Enabling the use cases:
4. apply suitable key hierarchy

› 4. Apply a suitable key hierarchy with key derivations

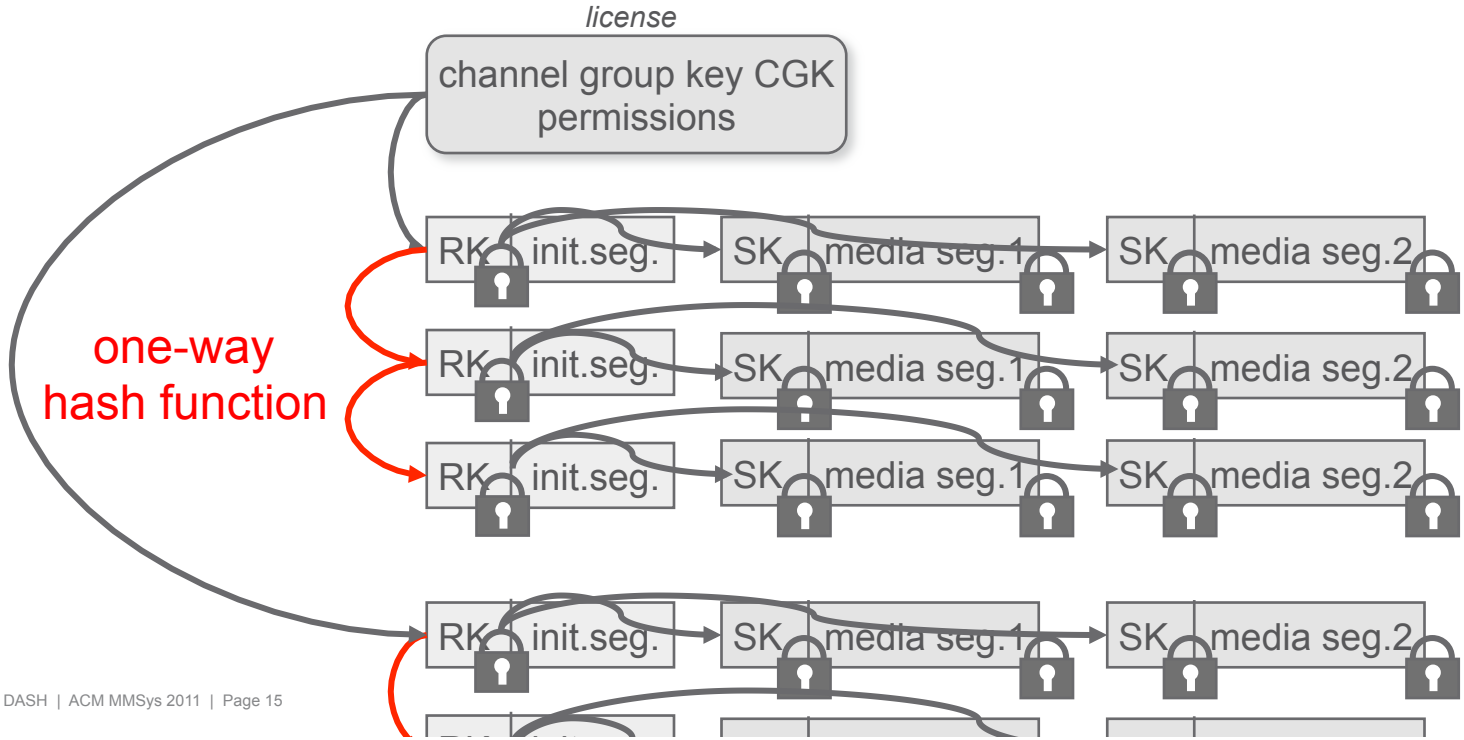
→ pay-per-maximum-quality



Enabling the use cases:
4. apply suitable key hierarchy

› 4. Apply a suitable key hierarchy with key derivations

→ pay-per-maximum quality per channel group

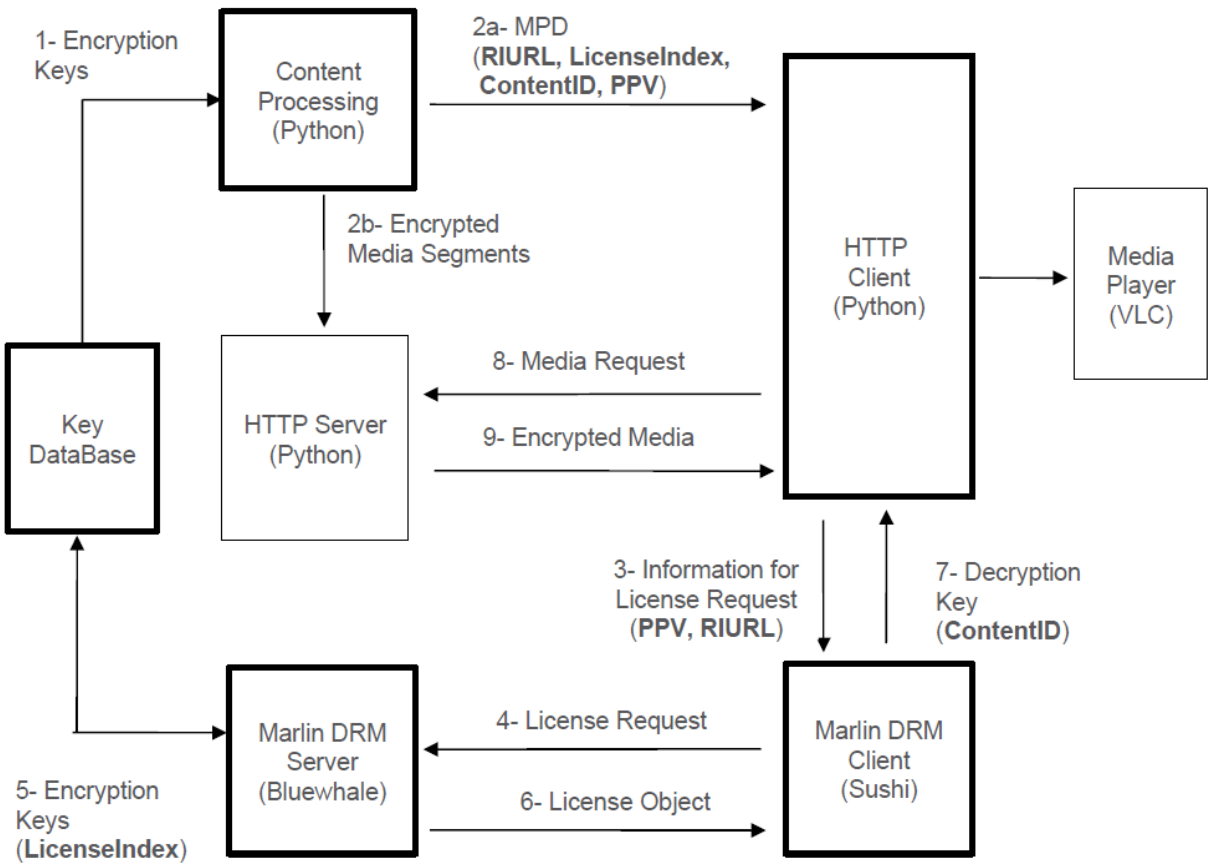


Marlin Broadband DRM

- Marlin Broadband
  - DRM system developed and driven by consumer electronics companies (Sony, Philips, Panasonic, Samsung)
  - Similar to other DRM systems
    - except rights expression: executable instead of XML
  - Adoption examples: Sony Playstation Network, Open IPTV Forum, YouView (aka Canvas), UltraViolet, Philips TV sets
  - We chose Marlin as DRM for a proof-of-concept implementation because reference software exists
  - Any other DRM would have been possible as well

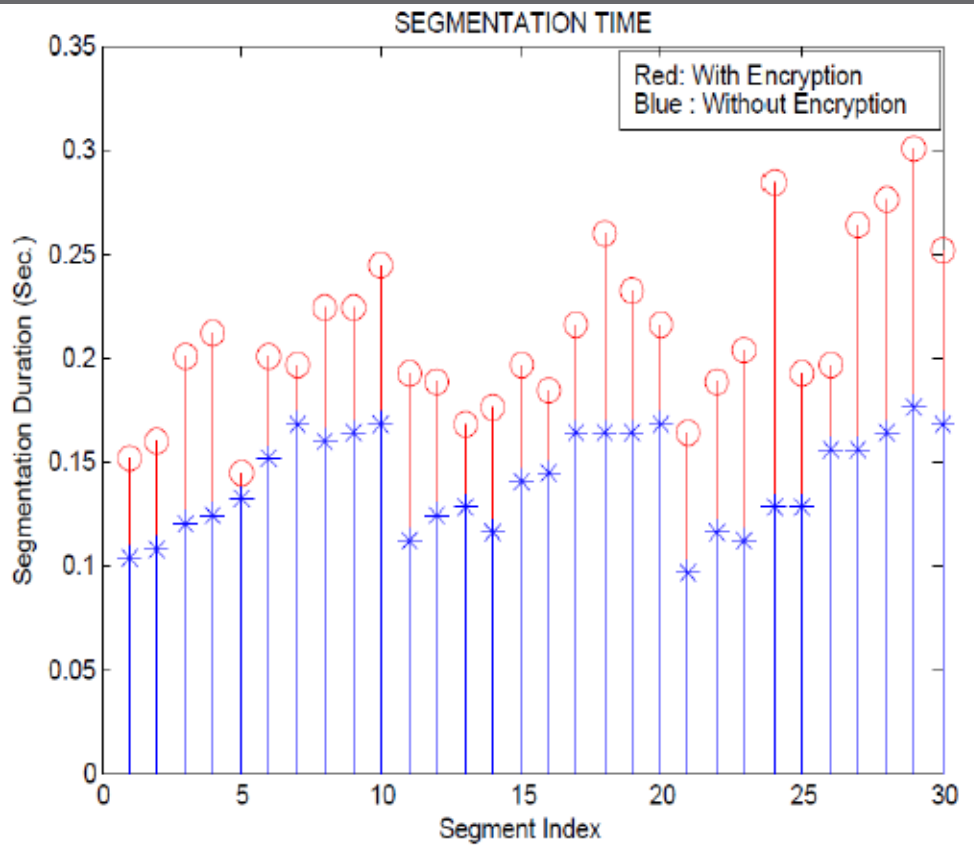
proof-of-concept

- All described extensions and use cases have been implemented as a PoC



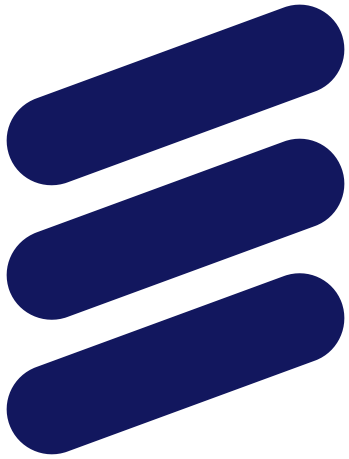
A note on Complexity

- Content preparation on experimental server with and without encryption
- Python based tools on standard PC
- Qualitative result: encryption does not add significant complexity
- → protected DASH is also possible for live content



Summary

- DASH: new media streaming paradigm with bright future
- DRM is in fact needed for premium video and certain business models
- DASH should support important use cases
- Current DASH does not
- We propose some extensions
  - more signaling in MPD
  - segment keys
  - suitable key hierarchy
- Proof-of-concept based on Marlin DRM has been implemented



ERICSSON