# ATSC 3.0 Content Protection

## MILE-HIGH VIDEO WORKSHOP

YASSER SYED AND GLENN REITMEIER

AUG 1, 2018

# Background

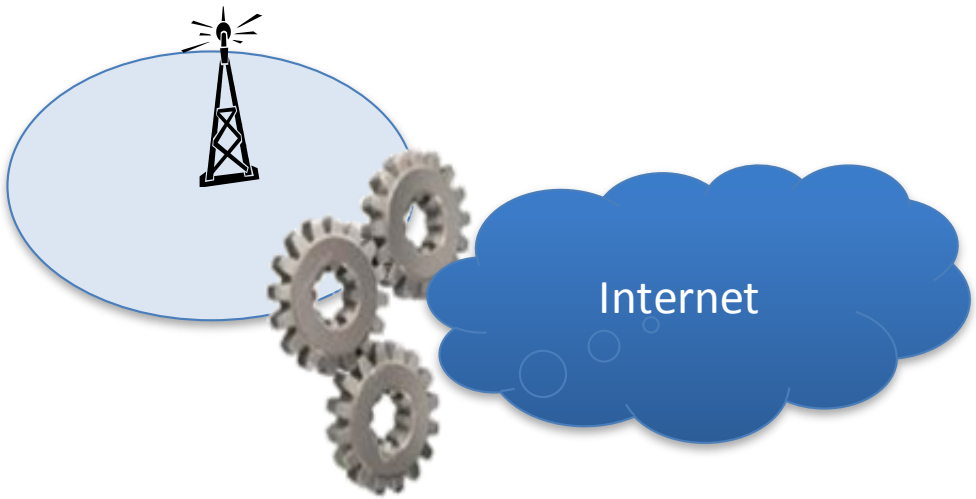
- ATSC 3.0 is the next-generation standard for over-the-air broadcasting
  - ATSC 3.0 is actually a suite of many standards, available at http://www.atsc.org
  - A/360 ATSC 3.0 Security and Service Protection
- Approved by the FCC in Nov 2017
- Voluntary market based transition for broadcasters, MVPDs and consumers
- Test stations on air
  - Phoenix: Pearl - NBCU – Fox – Univision - PBS
  - Dallas: Sinclair
  - Baltimore: Sinclair
  - Portland
- But what?!? – Content and Service Protection?!? Broadcasting is free (ad-supported) service

# Introduction

- FCC free-to-air requirement only applies to a TV Station's "Primary Program Stream"
- Beyond that, other uses are allowed, but revenue is subject to additional taxation
- FCC's ATSC 3.0 approval clarified that a broadcaster's primary stream must be free to viewers, not necessarily "in the clear" or an unencrypted transmission
- Inclusion of optional DRM in ATSC 3.0 gives broadcasters new protections and new business model opportunities

# Internet Protocol Data Format

## Broadcasting Becomes Part of the Internet




- Uses Internet Protocol - enable broadcasting to become PART OF the wireless internet
- Enables personalized and interactive content and targeted ads
- Easily retransmitted throughout home on WiFi
- With an ATSC 3.0 tuner, Broadcast IP streams complement 4G and WiFi
- **ATSC 3.0 is a broadcast AND broadband standard**
- Collaborative effort between DASH-IF and ATSC

# ATSC 3.0 Protocol Stack

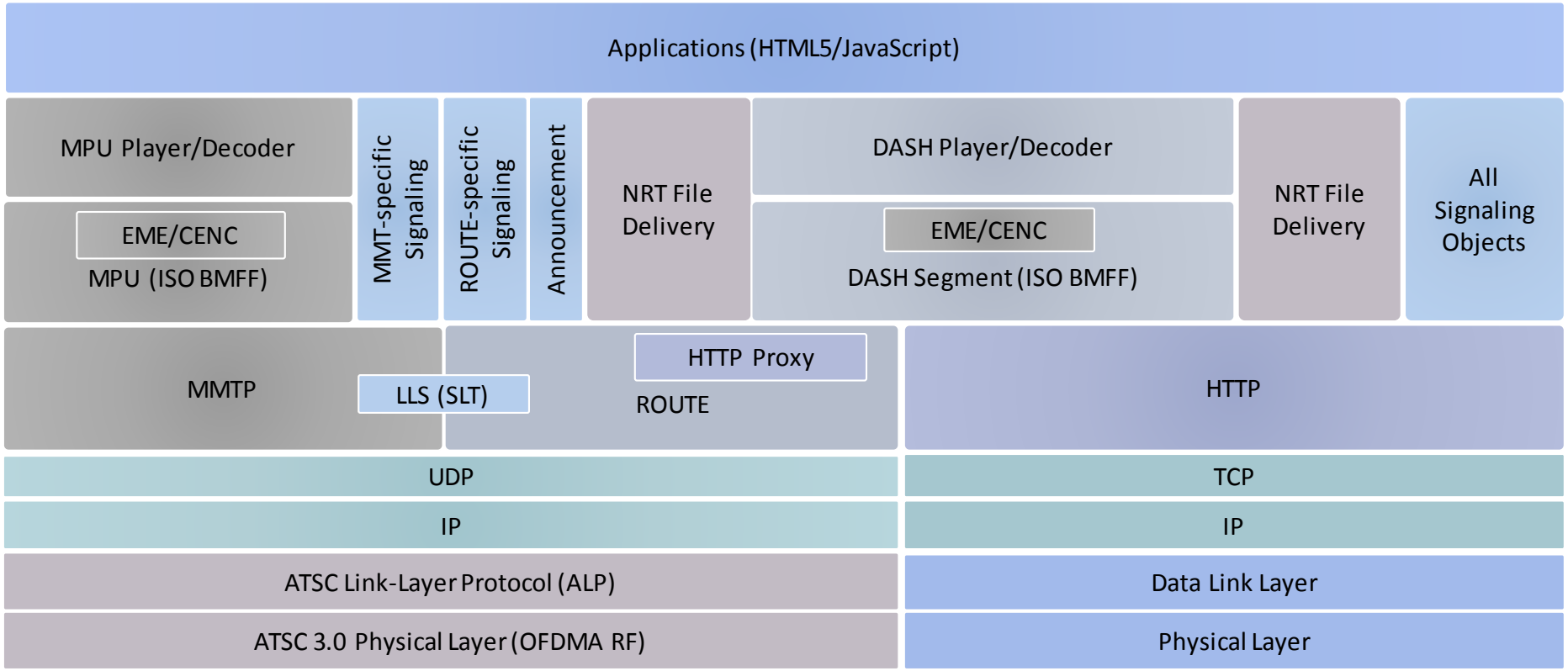
*ATSC 3.0 Makes Broadcasting Part of the Internet*

The ATSC 3.0 Management and Protocols Layer encompasses

- Service delivery and synchronization
- Service announcement and personalization
- Interactive services and companion screens
- Redistribution support / watermarks

IP Transport is used for broadcast delivery of both streaming and file content

***The use of IP transport is a game-changer for broadcasting***



# IP Broadcast Ecosystem Has New Threats

- IP-based broadcasting and smart receivers have the same vulnerabilities as any internet-based services and devices
- Need to protect integrity of broadcast – receiver ecosystem
- Need to protect content

## PKI & CAS/DRM

**PKI**

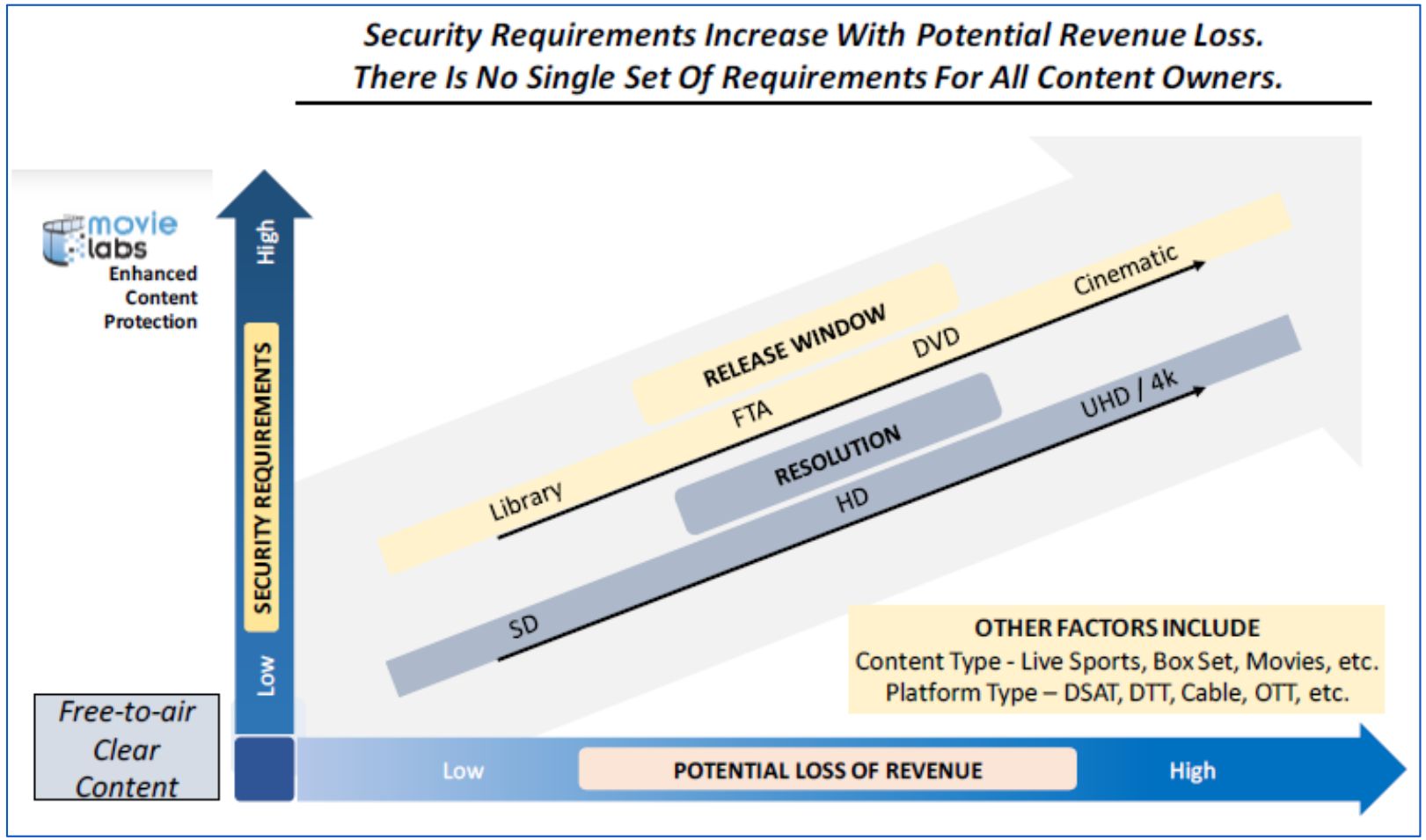
**Public Key Infrastructure**
Establishes trust between devices and broadcasters
Issues & validates Digital Certificates
**Protects against spoofing, hacking, signal intrusion**
Allows receivers to verify that the apps & signaling were broadcast by a trusted broadcaster and have not been changed.
Required - Specified in A/360 and A/331
required for signing signaling & apps

**DRM/CA**

**Digital Rights Management / Conditional Access**
**Encrypts** Content
**Protects against un-authorized viewing & re-distribution**
Issues rights, licenses and cryptographic keys
Optional – underlying technology specified in A/360

# Need For Content Protection

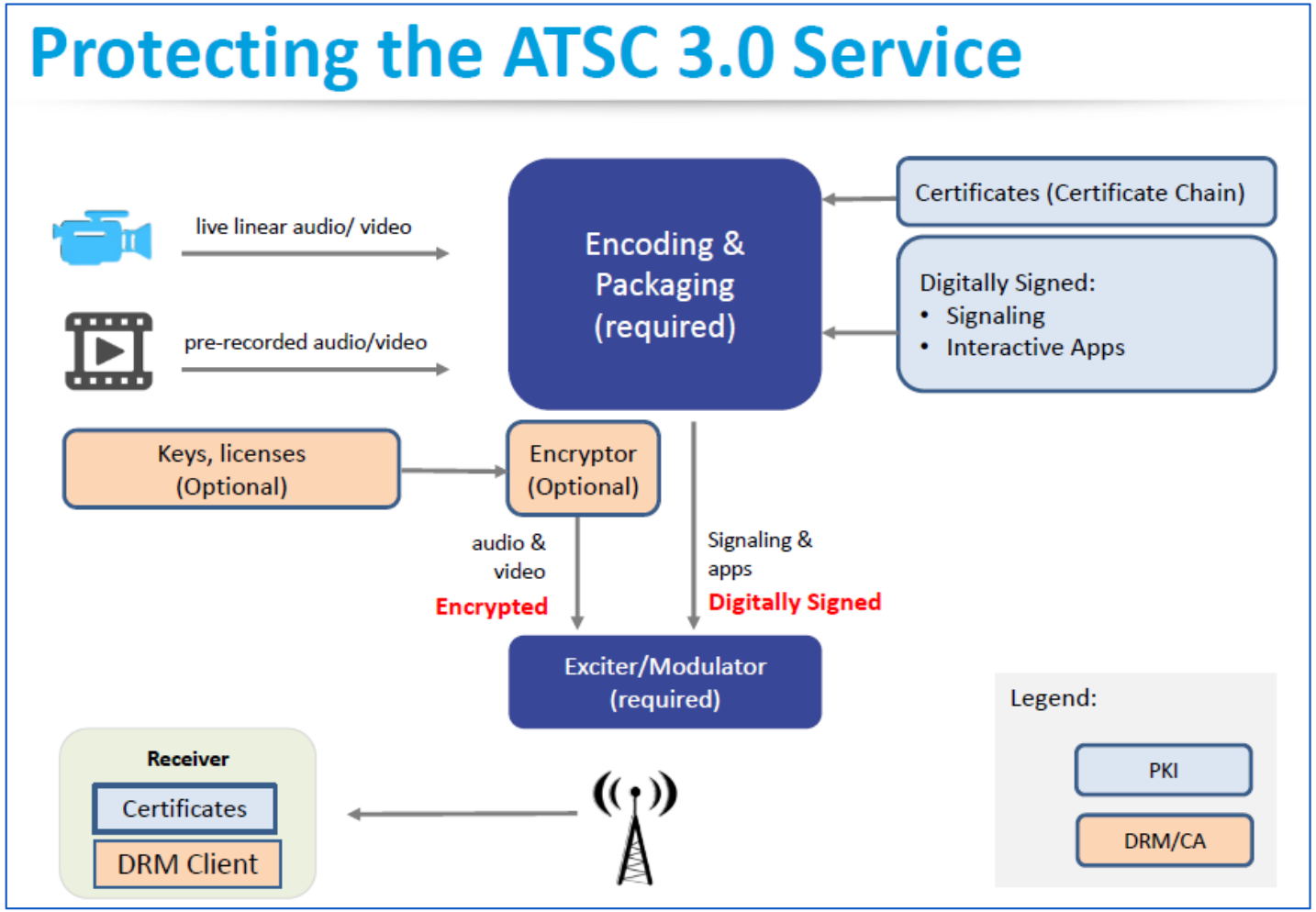
- UHD/HDR content will be a key part of ATSC 3.0 services
- Content Owners want higher security for higher quality content – MovieLabs Enhanced Content Protection spec
- Broadcasters (via the 3.0 standard) need to ensure that that they will qualify as a distributor of high-quality entertainment content




http://www.movielabs.com/ngvideo/MovieLabs%20Specification%20for%20Enhanced%20Content%20Protection%20v1.0.pdf

# A/360 Adopts Widely Used Web Technologies

- X.509 certificates
  - OCSP (Online Certificate Status Response) revocation
- MPEG Common Encryption (CENC)
  - Decouples content encryption from key acquisition
  - Enables industry use of multiple commercially available DRM systems
- W3C Media Source Extensions (MSE)
- W3C Encrypted Media Extensions (EME)



# Encrypted Track Structure

The IV (Initialization Vector) for every sample is provided as part of the sample auxiliary information in the “mdat” box or in the “senc” box together with information about the position of the encrypted chunks.

The license acquisition information is provided as part of the protection system specific header box “pssh”, where each DRM system is identified by a SystemID. The “pssh” box also provides a list of the provided Key Identifiers and opaque system-specific information that describes how to acquire the keys identified by the supported key ids.


**Figure 5.1** Encrypted Track structure - Storage of CENC related information.

# Box Structure – Encryption Metadata for Live Streams

The primary DRM related signaling components for use in ROUTE/DASH are:

1) The ContentProtection descriptor in the MPD which contains the URI for signaling of the use of Common Encryption or the specific DRM scheme.

2) Parameters of the 'tenc' box, carried as part of protection scheme information in the movie box ('moov') of the Initialization Segment, which specify encryption parameters and default_KID. The default_KID information may also be carried out-of-band in the MPD.

3) Signaling of common encryption sample auxiliary information in the form of initialization vectors and subsample encryption ranges, using the 'senc box as defined in ISO/IEC 23001-7, or via the SampleAuxiliaryInformationSizesBox ('saiz') and a SampleAuxiliaryInformationOffsetsBox ('saio').

4) 'pssh' license acquisition data or keys for each DRM system in a format that is protection system specific. 'pssh' refers to the Protection System Specific Header box as defined in ISO/IEC 23001-7, and which may be stored in the Initialization Segment or in Media Segments. It may also be present in a cenc:pssh element in the MPD. Note that while the presence of cenc:pssh information in the MPD increases the MPD size, it may allow faster parsing, earlier access, and addition of DRM systems without content modification.

5) Key rotation to enable modification over time in the entitlement for access to continuous live content. Details on how key rotation operates in the protection of broadcast DASH streaming content can be found in the DASH-IF Interoperability Points documents

A graphical representation of the box structure pertaining to encryption metadata support for live streaming content

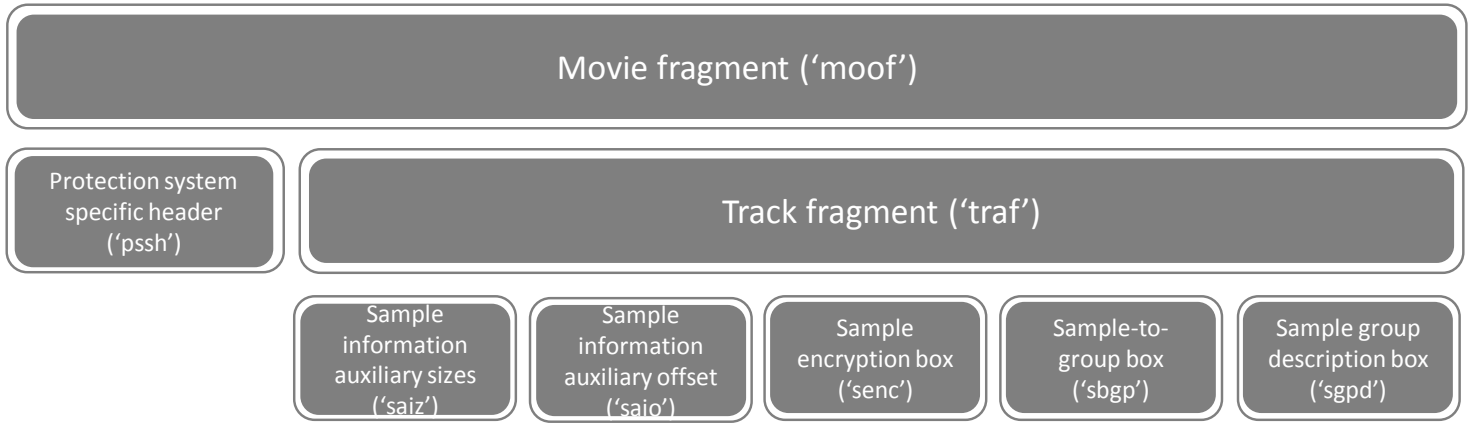



**Figure A.4** CENC-related metadata structure for protection of live streaming content.

# Encrypted Media Extensions (EME)

W3C Encrypted Media Extensions (EME) specifies JavaScript APIs which enable a web application to facilitate the exchange of decryption keys between a device-resident DRM system agent, referred to as the Content Decryption Module (CDM), and a key source or license server located somewhere on the network, to support the playback of encrypted audio and video media content.

EME is based on the HTML5 Media Source Extensions specification which enables adaptive bitrate streaming in HTML5 using, DASH-IF ATSC Profile with MPEG-CENC (Common Encryption) protected content.

The architecture of EME is shown, which depicts the primary interactions of the EME workflow between the functional entities involved in the detection of encrypted content and the subsequent acquisition of license and key material, to enable content decryption and playout

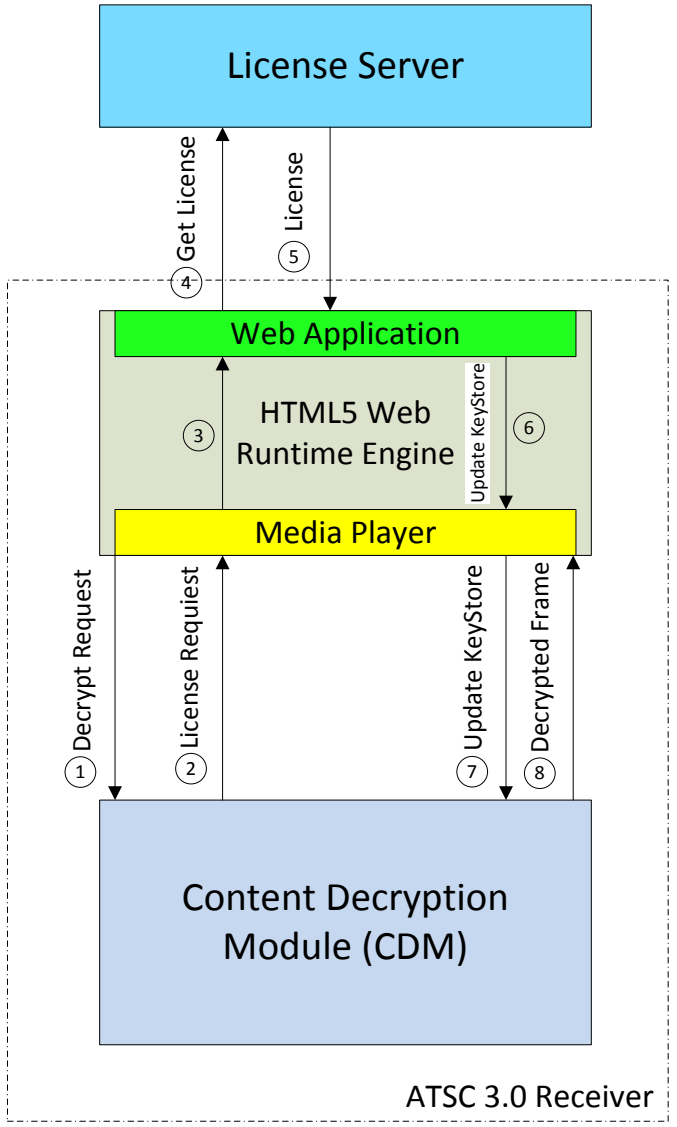



**Figure 5.2** Encrypted Media Extensions workflow.

# So “it’s the internet” – BUT…

- Prospective DRM providers must provide solutions that deal with:
  - MASSIVE scale of live broadcast events (e.g., the Super Bowl)
  - License distribution to intermittently-connected or never-connected receivers
  - License revocations on intermittently-connected or never-connected receivers
    - Blu-ray disc approach is to publish (broadcast) a revocation list”
  - Authorized re-transmission of broadcast signals by MVPD/OTT providers
- Work is in progress, so stay tuned…

# Summary and Ongoing Work

- ATSC 3.0 A/360 ATSC 3.0 Security and Service Protection is a transmission standard – it specifies the mechanisms that can be used, but not the specifics of implementations
- Enables use of commercially available solutions to establish PKI and to provide DRM
- Collaborative industry efforts among broadcasters and TV manufacturers are underway to
  - Establish a PKI for ATSC 3.0 receivers
  - Determine an initial set of DRMs that will be supported in receivers and can be used by broadcasters
  - Determine a set of 'Content Protection Use Cases' that satisfy network and broadcaster requirements and that can have appropriate licenses "baked in" during manufacturing

# Thank You

# APPENDIX

# A/360 Normative References


ISO/IEC: ISO/IEC 23001-7 Second edition 2015-04-01, "Information technology — MPEG systems technologies — Part 17: Common encryption in ISO base media file format files."
W3C: "Encrypted Media Extensions," W3C Recommendation 18 September 2017, World Wide Web Consortium, https://w3c.github.io/encrypted-media/.
W3C: "Media Source Extensions", W3C Recommendation 17 November 2016, World Wide Web Consortium, https://w3c.github.io/media-source/.
DASH: "Guidelines for Implementation: DASH-IF Interoperability Points for ATSC 3.0", Version 1.0, DASH Industry Forum, Beaverton, OR, 31 January 2017.
IETF: "RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," L. Bassham, W. Polk, R. Housley, Internet Engineering Task Force, Fremont, CA, April 2002.
IETF: "RFC 4033, DNS Security Introduction and Requirements," Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, Internet Engineering Task Force, Fremont, CA, March 2005.
IETF: "RFC 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," J. Schaad, B. Kaliski, R. Housley, Internet Engineering Task Force, Fremont, CA, June 2005.
IETF: "RFC 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments," A. Deacon, R. Hurst, Internet Engineering Task Force, Fremont, CA, September 2007.
IETF: "RFC 5077, Transport Layer Security (TLS) Session Resumption without Server-Side State," J. Salowey, H. Zhou, P. Eronen, H. Tschofenig, Internet Engineering Task Force, Fremont, CA, January 2008.
IETF: "RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2," T. Dierks, E. Rescorla, Internet Engineering Task Force, Fremont, CA, August 2008.
IETF: "RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," D. Cooper et al, Internet Engineering Task Force, Fremont, CA, May 2008.
IETF: "RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)," E. Rescorla, Internet Engineering Task Force, Fremont, CA, August 2008.
IETF: "RFC 5480, Elliptic Curve Cryptography Subject Public Key Information," S. Turner, D. Brown, K. Yiu, R. Housley, T. Polk, Internet Engineering Task Force, Fremont, CA, March 2009.
IETF: "RFC 5652, Cryptographic Message Syntax (CMS)," R. Housley, Internet Engineering Task Force, Fremont, CA, September 2009.
IETF: "RFC 5746, Transport Layer Security (TLS) Renegotiation Indication Extension," E. Rescorla, M. Ray, S. Dispensa, N. Oskov, Internet Engineering Task Force, Fremont, CA, February 2010.
IETF "RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.Message Specification," B. Ramsdell, S. Turner, Internet Engineering Task Force, Fremont, CA, January 2010.
IETF: "RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)," S. Turner, D. Brown, Internet Engineering Task Force, Fremont, CA, January 2010.
IETF: "RFC 5758, Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA," Q. Dang, S. Santesson, K. Moriarty, et al, Internet Engineering Task Force, Fremont, CA, January 2010.
IETF: "RFC 5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," H. Krawczyk, P. Eronen, Internet Engineering Task Force, Fremont, CA, May 2010.
IETF: "RFC 5940: Additional Cryptographic Message Syntax (CMS) Revocation Information Choices," S. Turner, R. Housley, Internet Engineering Task Force, Fremont, CA, August 2010.
IETF: "RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions," D. Eastlake 3rd, Internet Engineering Task Force, Fremont, CA, January 2011.
IETF: "RFC 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC)", S. Weiler, and D. Blacka, Internet Engineering Task Force, Fremont, CA, February 2013.
IETF: "RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP," S. Santesson, M. Myers, R. Ankney, et al, Internet Engineering Task Force, Fremont, CA, June 2013.
IETF: "RFC 8018, PKCS #5: Password-Based Cryptography Specification, Version 2.1," K. Moriarty, B. Kaliski, A. Rusch, Internet Engineering Task Force, Fremont, CA, January 2017.
IETF: "RFC 8446, TLS 1.3, The Transport Layer Security (TLS) Protocol Version 1.3," Internet Engineering Task Force, Fremont, CA, [July 2018].
IETF: "RFC 7539, ChaCha20 and Poly1305 for IETF Protocols," Y. Nir, A. Langley, Internet Engineering Task Force, Fremont, CA, May 2015.
ITU-T: "Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components", Rec. X.667, International Telecommunication Union, September 2004.