OMVC
OPEN MOBILE VIDEO COALITION

Report on

Service Protection and the Role of the Mobile DTV Trust Authority

A Guide for Broadcasters and Device Manufacturers

OMVC WHITEPAPER SERIES

Contents

This document is provided "as is" and without warranty of any kind. To the greatest extent Permitted by law, the open mobile video coalition ("omvc") disclaims all express, implied and statutory warranties, including, without limitation, the implied warranties of title, Noninfringement, merchantability, and fitness for a particular purpose. Omvc does not Warrant that this document is complete or without error and disclaims any warranties to the contrary. The user is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, standards, and specifications.

Introduction and Purpose

Mobile Digital Television (Mobile DTV) enables local television stations to deliver live, high-quality digital content to a wide range of ATSC-capable mobile and video devices, including mobile phones, portable media players, laptop computers, personal navigation devices and automobile-based "infotainment systems." With Mobile DTV, consumers can tune in to live, local news, traffic information, weather, sporting events or entertainment programs from the convenience of their car, at the beach—or wherever else they may be.

Mobile DTV is a scalable, spectrally efficient technology for distributing bandwidth-intensive mobile video to many users simultaneously. The service is “in-band”, meaning local broadcasters provide Mobile DTV services as part of their terrestrial transmission within the same, existing 6 MHz channel they use for their current ATSC digital television programming. Consequently, there is no need for stations to acquire additional spectrum to offer Mobile DTV services.

With minimal cost, broadcasters can transmit a robust Mobile TV signal by installing a Mobile DTV exciter and signal encoding equipment on existing TV transmission systems. Indeed, many of the broadcast transmission towers already have been retrofitted with equipment to deliver Mobile DTV signals to consumers.

Consumers have demonstrated a strong demand for Mobile DTV services. Through research conducted through consumer trials, OMVC found that consumers have a high level of excitement to be able to watch their favorite content in new situations and on new platforms, and consumers have expressed a high degree of satisfaction with the Mobile DTV experience. In addition, Mobile DTV is a highly reliable and efficient wireless communications system for delivering critical news and public safety information.

There is a clear need to make sure that broadcaster’s high-quality, digital content is made available to consumers in a protected and controlled manner. To this end, broadcasters, working through the OMVC, commissioned the establishment of an independent trust authority to administer the public key infrastructure (PKI) for Mobile DTV, which secures the transmission of information between broadcasters and mobile devices.

In 2011, the OMVC selected Nuestar Media to operate the Mobile DTV Trust Authority. In this capacity, Neustar generates and manages the certificates and keys necessary for the secure connection and use of the Mobile DTV service by connected personal digital devices. The Certificate Authority service that Neustar is providing is independent of, but will work with and is compatible with conditional access technologies.

This white paper summarizes how the PKI for Mobile DTV supports protection of broadcast services, as well as how the various participants in the Mobile DTV ecosystem interact.

The Open Mobile Video Coalition[1] (OMVC) is an alliance of U.S. commercial and public broadcasters formed to accelerate the development and rollout of mobile DTV products and services.

Relevant Standards and Industry Guidelines

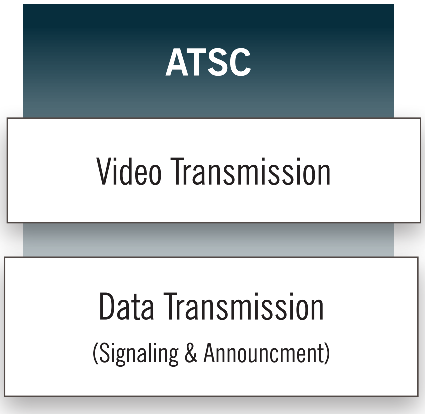
The Mobile DTV system relies primarily on two industry standard groups and one industry forum described below.

ATSC

ATSC-M/H (Advanced Television Systems Committee - Mobile/Handheld) is a standard in the USA for mobile digital TV that allows TV broadcasts to be received by mobile devices.

ATSC-M/H A/153 is modular in concept, with the specifications for each of the modules contained in separate parts.

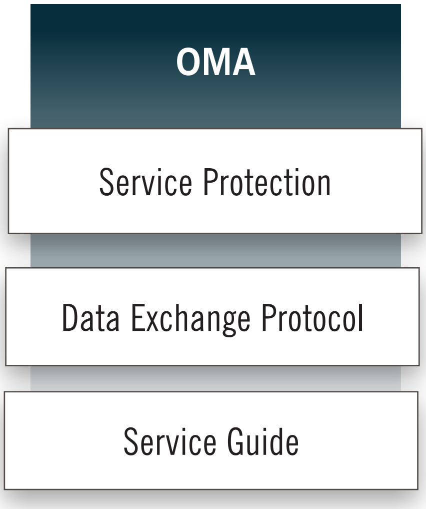
For the purposes of this white paper, the modules of interest are:



- Part 2: RF/Transmission System Characteristics [ATSC-1]
- Part 3: Multiplex and Transport Subsystem Characteristics [ATSC-2]
- Part 4: Announcement [ATSC-3]
- Part 6: Service Protection [ATSC-4]

OMA

OMA DRM (Open Mobile Alliance (OMA) Digital Rights Management) is a set of specifications, application level protocols and behaviors that provide transactional and life cycle management of content and applications on mobile devices.



[1] www.omvc.org

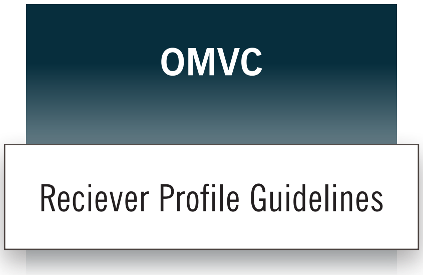
OMA BCAST - Open Mobile Alliance (OMA) Mobile Broadcast Services Enabler Suite (BCAST) is an open global specification for mobile TV and on-demand video services which can be adapted to any IP-based mobile and P2P content delivery technology.

For the purposes of this white paper, the OMA specifications of interest are:

- Digital Rights Management 2.0 [OMA-1] (includes requirement for a PKI)
- Service and Content Protection [OMA-2]
- Service Guide [OMA-3]
- Broadcast Extensions [OMA-4]

OMVC

The OMVC (Open Mobile Video Coalition) has created Receiver Profile Guidelines [OMVC-1] that provide directional guidance to consumer electronics manufacturers on the device features and functionalities that will help ensure that devices have robust reception capability and interoperability with services offered by broadcasters.



OMVC

Reciever Profile Guidelines

Conditional Access

The ATSC A/153 Mobile DTV standard incorporates a Conditional Access System (CAS) that is based on the OMA-DRM standard. For the purposes of this white paper, the Conditional Access System provides the mechanism to secure the transmission of information between broadcasters and mobile devices, otherwise known as Service Protection.

Typical MDTV Broadcast Infrastructure

- Encoder/Scrambler/Streamer – This system encodes the content in a format suitable for Broadcast and usable by a mobile terminal. It also encrypts the resulting stream on the fly and streams it.
- Content Management System (CMS) – This system manages the schedule and the products defined on it. The CMS provides Product references to the Subscriber Management System so that they can be offered to the subscribers.
- Electronic Service Guide (ESG) – Program and system information for ATSC M/H.

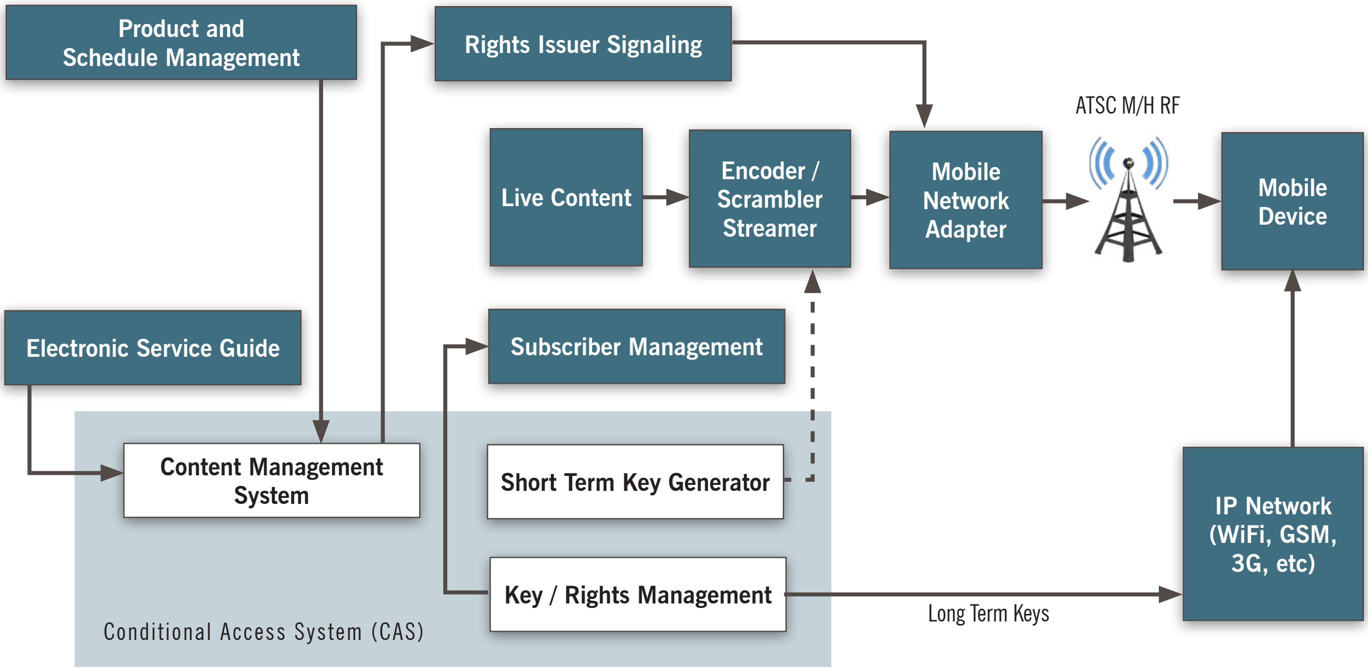


Figure 1
Broadcast Infrastructure with Conditional Access

- Rights Issuer Signaling – This system provides basic information, the logical structure of the transmitted services and the decoding parameters for video and audio.
- Mobile Network Adaptor – This system handles the task of multiplexing existing ATSC streams with incoming mobile IP stream. This component may also include a Single Frequency Network processor.
- Subscriber Management System (SMS) – This system maintains a central database of the Broadcaster's users and facilitates commercial transactions with the user. The SMS also and interacts with the CAS to enforce the subscriptions.

Typical Conditional Access Components

- Product & Schedule Management (PSM) – Imports the schedule & product information from the CMS and assigns Service Key IDs which are signaled to devices according to the OMA BCAST specifications. In the event that the Content Management System is not available, the PSM may provide an optional user interface to define the Services and Products[2].

[2] This feature is vendor-dependent

- Key/Rights Management System – Manages and maintains authorizations for each users/ subscribers. Depending upon the vendor, it might offer an interface to the operator's SMS through which it is possible to activate or cancel subscriptions.

- Short Term Key Generator– Generates the STKM containing the current Traffic Encryption Key (TEK) and other required information and returns it to the Scrambler for delivery with the content. The interface between the Short Term Key Generator and the Broadcast equipment is standardized by DVB, in the DVB SimulCrypt specification [ETSI-1].

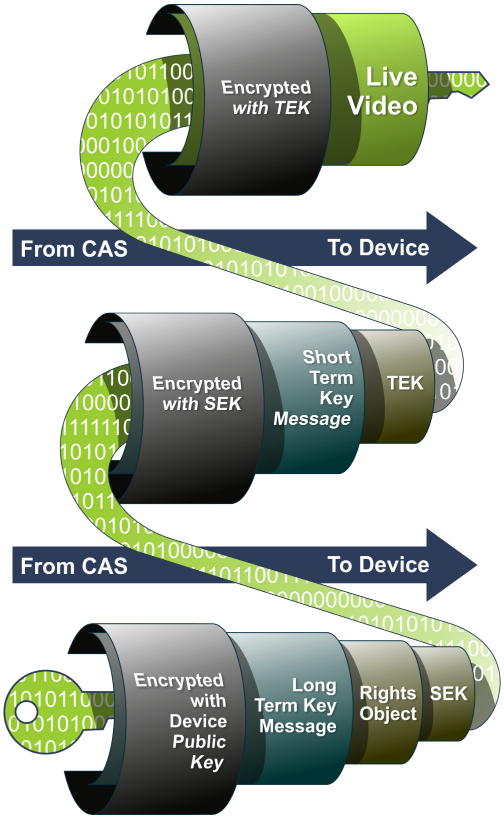


Figure 2
Multiple Layers of Encryption

OMA DRM Important Concepts

- Live Video streams are encrypted with a Traffic Encryption Key (TEK) – often referred to as a Short Term Key
  - TEKs typically change every 10 seconds
- Encrypted TEK are sent to devices in ATSC M/H RF broadcast streams
  - A packet called Short Term Key Message (STKM) contains the TEK
  - STKM are encrypted with a Service Encryption Key (SEK) – often referred to as a Long Term Key
  - SEK typically changes every 7 to 14 days
  - The device needs to know the SEK to get the TEK from the STKM and then descramble the stream
- The device gets the SEK in an object called Right Object, packaged in a Long Term Key Message (LTKM)
  - When the user purchases new channels, or before the SEK expires, the device needs to receive a new Right Object (RO)
  - The RO is specific for each device (based on certificate) and contains the SEK

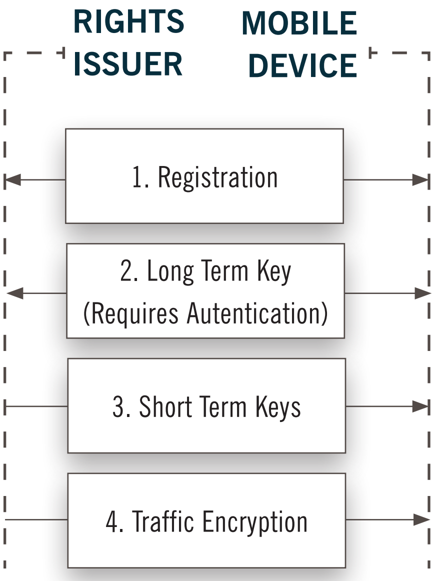


Figure 3
OMA 4-Layer Cryptographic Protocol

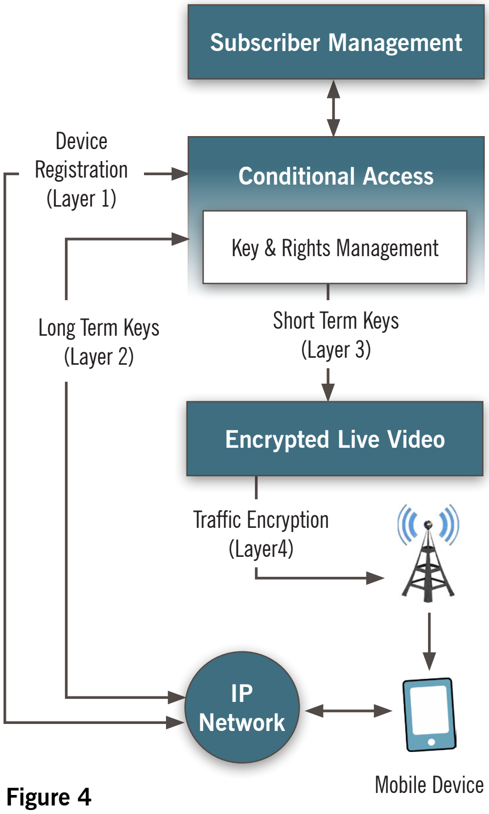


Figure 4
Conditional Access and Key Delivery

4-Layer Cryptographic Protocol

OMA specifies a 4-layer cryptographic protocol which is the basis for service protection:

1. Registration. A device must first register with the Rights Issuer and establish itself as a trusted entity. The registration process is a two-way exchange of information over a secure IP connection using Transport Layer Security (TLS) [IETF-1] as specified by OMA BCAST [OMA-3]. The device initiates the registration process via a 'hello' message.
2. Long Term Key Exchange. The Long Term Keys are only sent to the device after Registration and also depends upon authentication of the device by the exchange of digital certificates via TLS. The device initiates the long term key exchange via a '"Service Request" or "LTKM Renewal Request" message as defined in [BCAST10-Services].
3. Short Term Key Exchange. Short Term keys are sent in the broadcast stream and are encrypted with the Long Term Keys.
4. Traffic Encryption. Live Video traffic is also sent in the broadcast stream and is encrypted with Short Term Keys.

Figure 3 (shown on the left) illustrates how the 4 layer protocol is applied in practice.

For more detail on the interactions involved in the 4 layer protocol, please see 'Interactions between Devices and Rights Issuers' elsewhere in this document.

Typical CAS Deployment Options

Fully centralized Architecture

The simplest deployment architecture involves a centralized Head End, where the Conditional Access System and other ancillary systems are located. Please see below.

Remotely located scramblers receive their keys through a VPN connection to the centralized Head End.

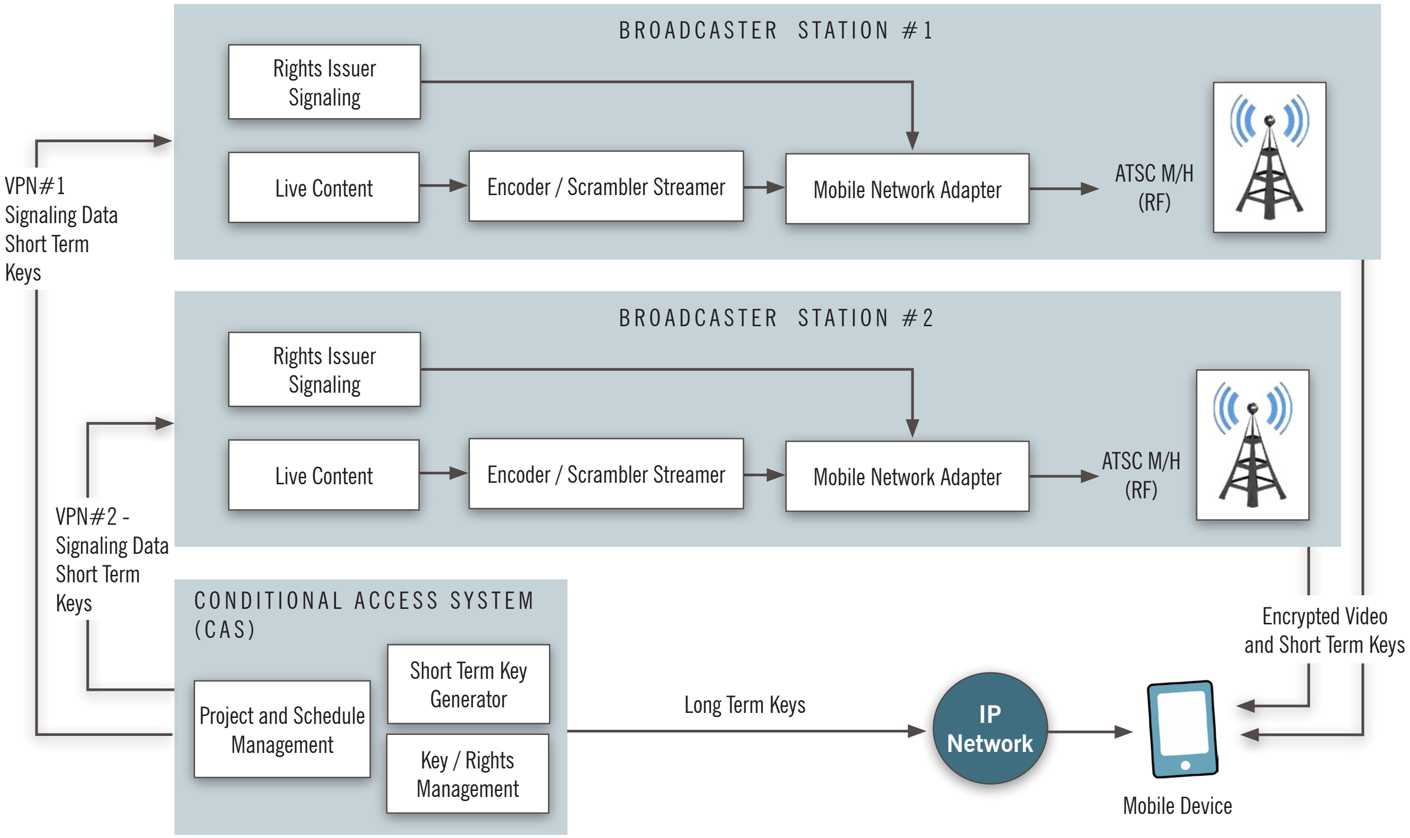


Figure 5
Fully Centralized Architecture

Centralized Key management with local STKM Generators

Another option is to distribute the Short Term Key generation function. The principle is similar in all other aspects, however Short Term Keys are locally generated within the broadcast station which manages the distributed functions from the centralized Head End.

Advantage: This option is more robust in that it minimizes the impact of network issues that could affect a scrambler's ability to receive Short Term Keys.

Disadvantage: This option requires additional cost in terms capital equipment to supply the distributed hardware for Short Term Key generation.

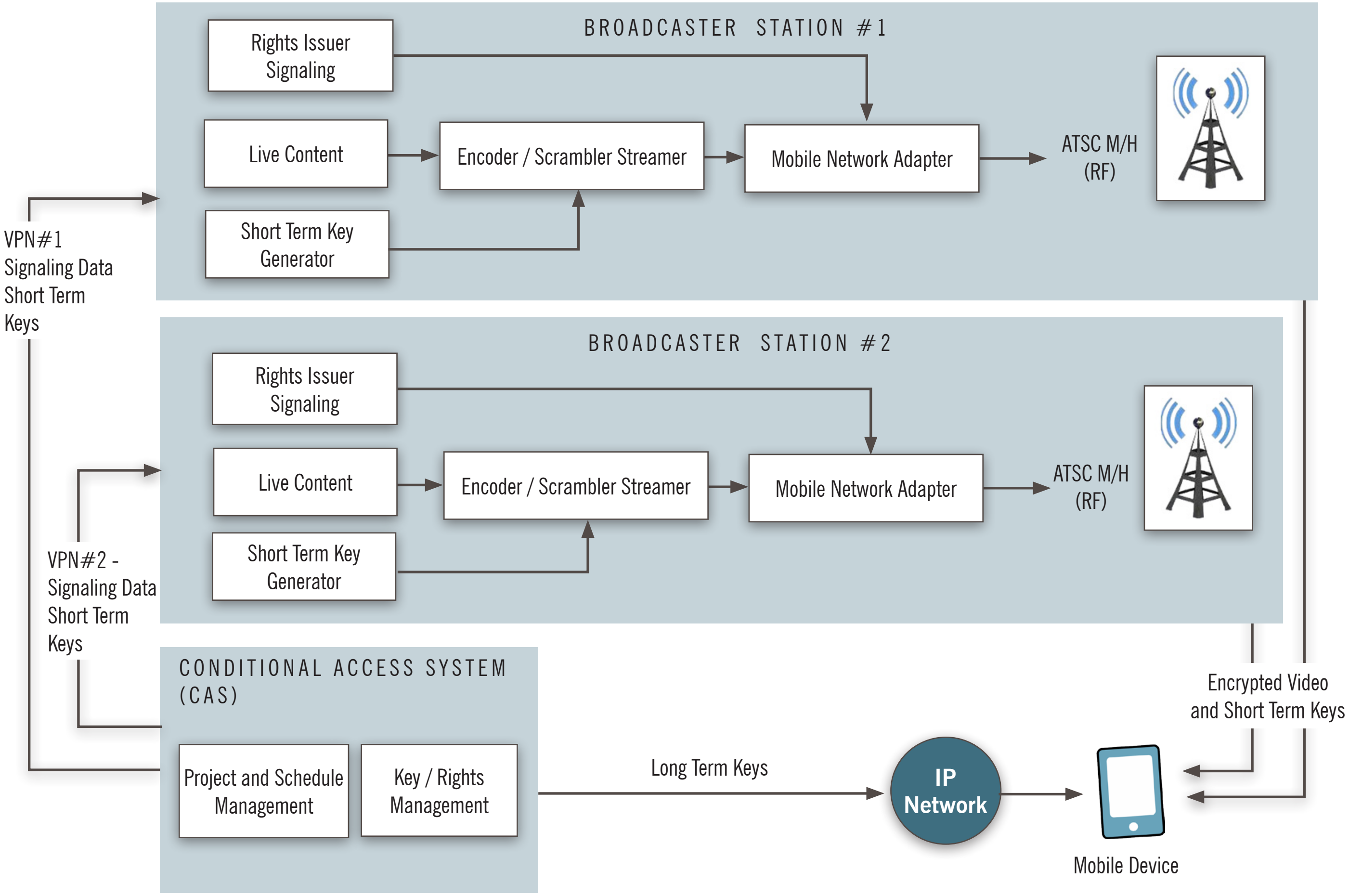


Figure 6
Centralized Key Management with Local Short Term Key Generation

The Mobile DTV Ecosystem

The Mobile DTV Ecosystem includes the following functional groups:

Broadcasters

Mobile DTV Broadcasters supply content in the form of live video over ATSC M/H transmission. Each broadcaster may provide multiple TV channels.

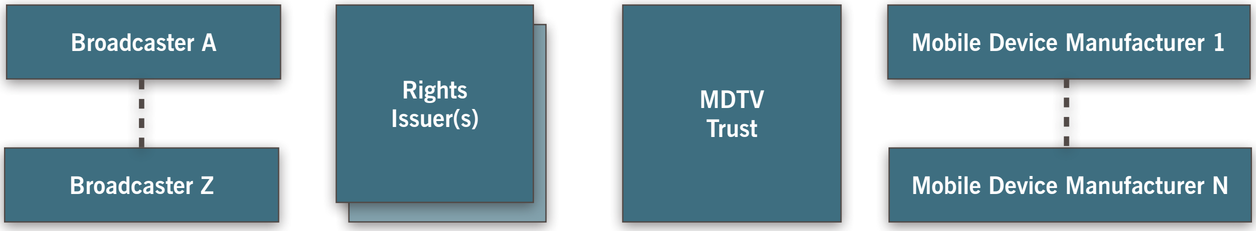


Figure 7
Mobile DTV Ecosystem

Rights Issuers

A Rights Issuer is an entity that operates the conditional access system(s) which issue short and long term keys to devices for the purpose of protecting broadcasted content. While neither OMA nor the ATSC specify the number of rights issuers or specific implementation architecture, in practice it is anticipated that one Rights Issuer will provide service protection services for one or more broadcasters.

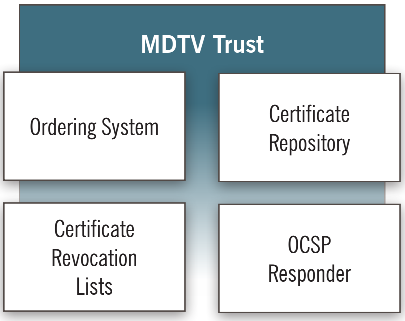


Figure 8
Mobile DTV Trust Components

Mobile DTV Trust

The Mobile DTV Trust is an independent organization which provides the public Key Infrastructure (PKI) which allows mobile devices and DTV service providers to connect seamlessly and securely.

The key elements of the PKI include:

Ordering System

The Certificate Repository provides the capability for Rights Issuers and Device Manufacturers to securely order and receive digital certificates and monitor activity via reports.

Certificate Repository

The Certificate Repository is a centralized, secure storage of digital certificates which maintains current status of certificates in the ecosystem.

Certificate Revocation Lists (CRLs)

CRLs are time-stamped lists of all revoked certificates.

Online Certificate Status Protocol (OCSP) responder

An OCSP responder is a system which responds to real time queries about the revocation status of a digital certificate.

Certificate Hierarchy

The Mobile DTV Trust operates a hierarchy of certificate authorities as described below.

Root Certificate Authority

The Root Certificate Authority (CA) issues the Root certificate (which is self-signed) and is the top-most certificate of the tree, the private key of which is used to “sign” other certificates. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate.

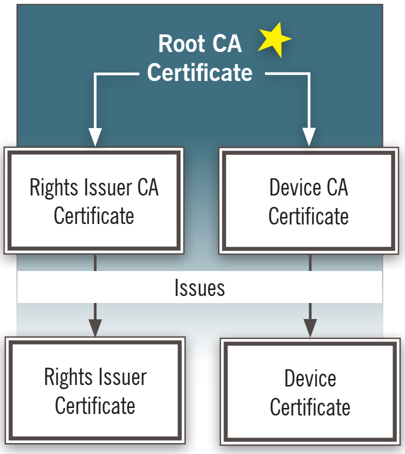


Figure 9
Certificate Hierarchy

Rights Issuer Certificate Authority

The Rights Issuer Certificate Authority issues Rights Issuer Certificates, which are digitally signed using its private key. All Rights Issuer Certificates inherit the trustworthiness of the CA certificate.

Device Certificate Authority

The Device Certificate Authority issues Device Certificates, which are digitally signed using its private key. All Device Certificates inherit the trustworthiness of the CA certificate.

To use certificates for security, the authenticity and validity of each certificate received must be verified. This verification depends upon the concept of trust and the delegation of trust.

A certificate chain consists of all the certificates needed to certify the subject identified by the end certificate. In practice this includes the certificates of intermediate Certificate Authorities, and the certificate of a root CA trusted by all parties in the chain. Every intermediate Certificate Authority in the chain holds a certificate issued by the CA one level above it in the trust hierarchy. The Root Certificate Authority issues a certificate for itself.

Mobile Device Manufacturers

Mobile Device Manufacturers supply commercial devices which are cable of receiving ATSC M/H signals per the OMVC Receiver Profile Guidelines. As illustrated in Figure 4 above, many device manufacturers are anticipated in the Mobile DTV ecosystem.

OMA and ATSC do not require or suggest any specific architecture or implementation for mobile devices, other than requiring they conform to the OMA-DRM Profile based upon the BCAST specifications. However, most devices will require many of the functions listed below in order to receive and play encrypted video[3].

- ATSC M/H Receiver to provide RF transmission reception, channel tuning and other basic functions such as demodulation, error correction, decompression and Audio/Video synchronization.

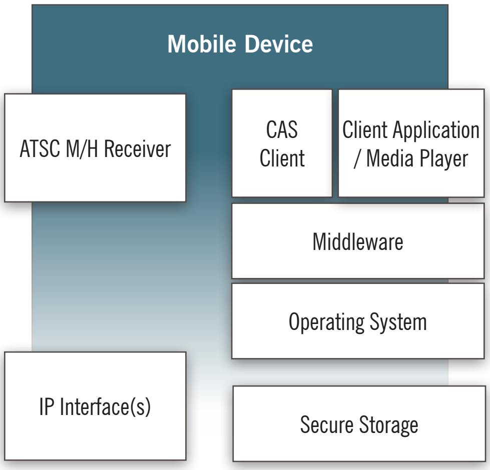


Figure 10
Mobile Device Components

- Secure Storage for certificates and protected keys.
- Operating System provides common services for application software.
- Conditional Access Client handles key processing.
- Middleware provides software libraries so that client software does not need to concern itself with variations between differwent device types.
- Client Application and/or Media Player provides the user interface which controls and displays video.

Rights Issuers and the Mobile DTV Trust

In order for a Rights Issuer to protect information during the delivery to a mobile device, they must obtain the following from the Mobile DTV Trust Authority:

Rights Issuer (RI) Certificate

This is an X.509 digital certificate that includes important information such as

- Certificate Serial Number
- Name of the entity that owns the certificate
- Validity Period (either 2 or 3 years)
- Signature (SHA-256)
- RI's public Key. This is shared with mobile devices and is used to encrypt information sent by the device during parts of the 4 layer cryptographic protocol described above.

[3] How a given manufacturer or vendor designs and implements a solution will vary

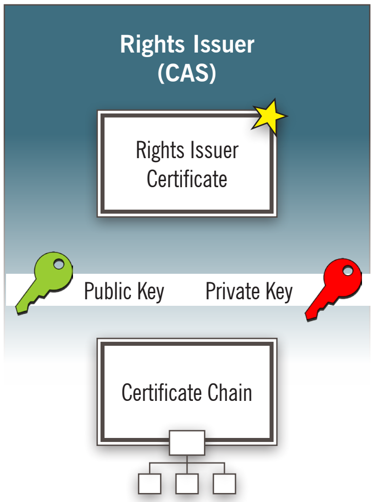


Figure 11

Items a Rights Issuer receives from the Mobile DTV Trust

- Subject Key Identifier. This is a cryptographic hash of the public key, and is used as the RI ID[4] when identifying a specific Rights Issuer to a device.

RI's Private Key

This is used by the Conditional Access System to decrypt information sent from the device during parts of the 4-layer cryptographic protocol described above. The RI Private Key is 2048 bits (256 bytes) long.

Certificate Chain

This is sent by the Conditional Access System to the device so it can verify the other certificates in the PKI hierarchy (RI Certificate Authority and the Mobile DTV Root).

Ordering and Receiving RI Certificates from the Mobile DTV Trust

1. Establish service with Neustar via Service Agreement.
2. Complete the registration documentation. This documentation specifies contact information for users of the online ordering system: authorized 'requestors' and 'approvers'.
3. Neustar notifies users (requestors, approvers) of user ID and password.
4. Users obtain 'User Certificates' which authenticate them with the ordering system.
5. Users install their user certificates.
6. Requestors log in and request certificates.
7. Requestors also download the certificate chain which will be installed on their Conditional Access System(s).
8. Approvers are notified of new request(s); they log in and approve the requests.
9. Requestors are notified of approval; they log in and download certificate bundle (certificate and the corresponding private key is contained in a file in Public-Key Cryptography Standard #12 format).

[4] [OMA-1] page 32

Utilizing the Rights Issuer Certificate and Certificate Chain

The Rights Issuer certificate and private key are installed (along with the certificate chain) on the Conditional Access System server per the Operations, Administration and Maintenance Procedures (OAM&P) of the Conditional Access System vendor.

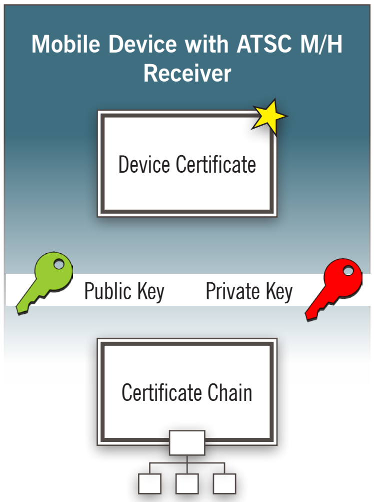


Figure 12

Items Device Manufacturers receive from the Mobile DTV Trust

Device Manufacturers and the Mobile DTV Trust

In order for devices to protect information during the delivery to a mobile device, they must receive and install the following on each device.

Device Certificate

This is an X.509 digital certificate that includes important information such as:

- Certificate Serial Number
- Manufacturer Name
- Validity Period (30 years)
- Device's Public Key. This is used by the RI to decrypt information sent by the device during parts of the 4-layer cryptographic protocol described above
- Subject Key Identifier. This is a cryptographic hash of the public key, and is used as the PKI Device ID[5] when identifying an individual device with conditional access systems

Device's Private Key

This is used by the device to encrypt information sent to the RI during parts of the 4-layer cryptographic protocol described above. The device's private key is either 2048 bits (256 bytes) or 1024 (128 bytes) long.

Certificate Chain

This is sent by the device to the Rights Issuer's Conditional Access System so that it can verify the other certificates in the PKI hierarchy (Device Certificate Authority and the Mobile DTV Root).

[5] [OMA-1] page 30

Ordering and Receiving Device Certificates From the Mobile DTV Trust

1. Establish service with Neustar via Service Agreement.
2. Complete the registration documentation. This documentation specifies contact information for users of the online ordering system: authorized ‘requestors’ and ‘approvers’.
3. Neustar notifies users (requestors, approvers) of user ID and password.
4. Users obtain ‘User Certificates’ which authenticate them with the ordering system.
5. Users install their user certificates.
6. Requestors log in and request certificates.
7. Requestors also download the certificate chain which will be installed on their Conditional Access System(s).
8. Approvers are notified of new request(s); they log in and approve the requests.
9. Requestors are notified of approval; they log in and download certificate bundle (certificate and the corresponding private key is contained in a file in Public-Key Cryptography Standard #12 format).
10. The certificate chain includes the Device Certificate Authority certificate as well as the MDTV Root certificate. This information is downloaded in Privacy Enhanced Mail Base 64 (.pem) format.
11. Requestors are notified of approval; they log in and download certificate bundles.

Each certificate and the corresponding private key are contained in a file which is Public-Key Cryptography Standard #12 format.

Certificates ordered in bulk will be bundled in a compressed and encrypted package.

Installing Device Certificates

At the time of manufacture, the following items are to be installed on each device in a secure area of non-volatile storage which is protected from tampering or unauthorized access:

- One unique certificate and corresponding private key provided by Neustar
- Certificate chain of the device provided by Neustar

Commonly used Unix tools such as 'openssl' are required to extract, encrypt and install Device Certificates and keys on protected storage.   There are no proprietary tools or methods necessary.

While OMA and ATSC documents only specify that the device private key be protected from unauthorized access, the OMVC recommends keys to be DER (Distinguished Encoding Rules) encoded then encrypted and/or obfuscated such that only authorized applications may access it.

Note: The MDTV Trust has published a Certificate Policies for both Devices [PKI-1] and Rights Issuers [PKI-2] which outline proper usage of certificates.

Interactions Between Devices and Rights Issuers

The interactions described below have been simplified for the purposes of this white paper. Please refer to [OMA-1] , [OMA-2] and [OMA-3] for more detail.

Channel Scan

Mobile Device enters broadcast area and discovers ATSC M/H signal.

The Mobile Device receives Service Map Table(s) through the broadcast transmission which contains the Rights Issuer Uniform Resource Identifier[6] (URI – the location of Conditional Access System) for the ensemble which signaled.

Device Registration

The registration process is required only once per Conditional Access System.

The registration process is first layer in the cryptographic architecture specified by OMA; it authenticates the device with the conditional access system, and paves the way for short and long term key exchange.

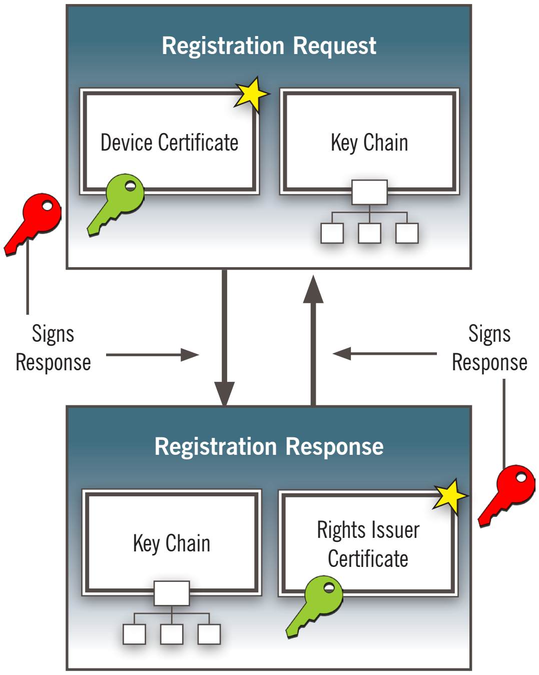


Figure 13
Registration Request and Response

[6] [ATSC-2] p66

A. Device sends registration request to the URI of the Rights Issuer's Conditional Access System using HTTPS[7]

   - The registration request includes the Device's certificate (which includes the Mobile DTV Device ID) and associated certificate chain; the data is digitally signed by the device using its private key.

B. Rights Issuer Conditional Access System verifies the digital signature on the request, and then must perform an OCSP transaction on behalf of the device to verify the status of the Rights Issuer Certificate. (Not shown)

C. Rights Issuer Conditional Access System responds to the registration request

   - The response includes the Rights Issuer's certificate (which contains the Mobile DTV Rights Issuer ID) and associated certificate chain; the data is digitally signed by the Rights Issuer's Conditional Access System using the Rights Issuer's private key.

D. The Device verifies the digital signature on the request using the RI public key

Service Provisioning

Service provisioning is the second layer in the cryptographic architecture defined by OMA. The Rights Issuer periodically (every 7-14 days, which is considered 'long term') changes the Keys which provide access to broadcast services. These are called Service Encryption Keys (SEK). Note that all of the transactions for Service Provisioning are using HTTPS.

A. Device requests keys (or updates to keys) for access to a broadcast service. This is made via an LTKM Renewal Request Message which is sent to the URI of the Rights Issuer's Conditional Access System in the form of a Rights Object Request.

   - The request includes the Mobile DTV Device ID (hash of the device's public key) as well as the Rights Issuer's ID (hash of the Rights Issuer's public key – 'RI ID') which the device received in the registration request.

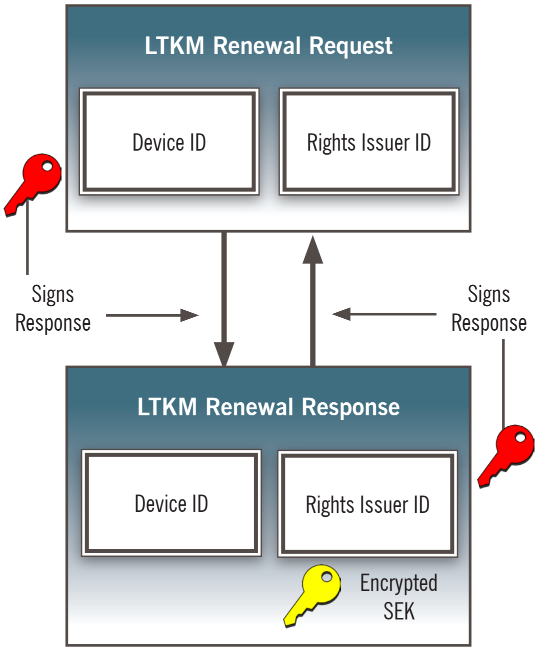


Figure 14
Long Term Key Request/Renewal

[7] HTTPS is a combination of HTTP with TLS 1.0 or higher protocol, which conforms to [OMA-2] and [ATSC-5]

B. Rights Issuer Conditional Access System verifies

- The digital signature on the request
- That the RI ID matches the hash of its public key
- That the Mobile DTV Device ID has already registered by comparing it to a database of IDs acquired during successful registrations.

C. The Rights Issuer's Conditional Access System encrypts the SEK using the public key of the device.

D. The Rights Issuer's Conditional Access System responds to the device via an LTKM Renewal Response Message in the form of a Rights Object Response.

- The response includes the Mobile DTV Device ID, the Rights Issuer ID (RI ID) and a Rights Object which contains the encrypted SEK.

E. The device receives the LTKM Renewal Response and decrypts the SEK using its private key.

Receiving and Un-Encrypting Broadcast Video

A. The Rights Issuer's Conditional Access System creates new Traffic Encryption Keys (TEKs) approximately every 10 seconds and sends them to the broadcaster's Encoder/Scrambler/Streamer via DVB Simulcrypt [ETSI-1].

(Please refer to Figure 2 Multiple Layers of Encryption above for more detail on the encryption of TEKs.)

B. The broadcaster's Encoder/Scrambler/Streamer encrypts live video content using TEKs received from the Rights Issuer's Conditional Access System and sends the encrypted live video over the air via ATSC M/H RF transmission.

- The broadcaster's Encoder/Scrambler/Streamer also sends updated TEKs which have been encrypted with the SEK and sends them over the air in messages called Short Term Key Messages.

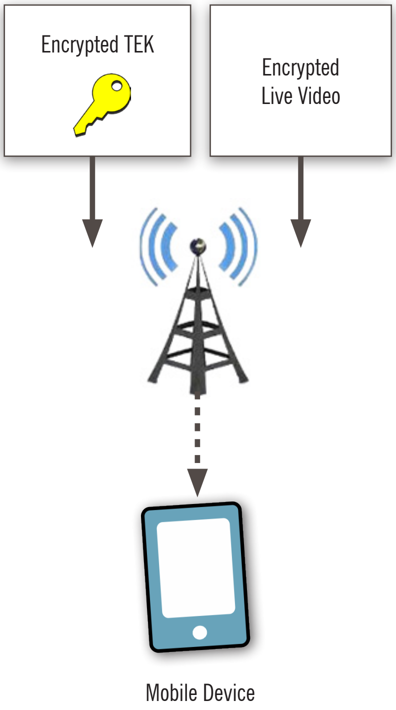


Figure 15
Short Term Key (TEK) Delivery

C. Devices receive encrypted TEKs over the broadcast ATSC M/H RF Transmission and decrypt them using the SEK received during Service Provisioning.

- Devices use the TEKs to decrypt the video which is also received over the air via ATSC M/H RF Transmission.

Glossary

ATSC	Advanced Television Systems Committee
ATSC M/H	Advanced Television Systems Committee – Mobile/Handheld
BCAST	BroadCAST services enabler suite
CA	Certificate Authority
CAS	Conditional Access System
CMS	Content Management System
DER	Distinguished Encoding Rules
DTV	Digital Television
DVB	Digital Video Broadcast
LTKM	Long Term Key Message
OAM&P	Operations, Administration, Maintenance and Provisioning
OCSP	On-Line Certificate Stats Protocol
OMA	Open Mobile Alliance
OMVC	Open Mobile Video Coalition
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSM	Product and Schedule Manager
RF	Radio Frequency
RI	Rights Issuer
SEK	Service Encryption Key
SFN	Single Frequency Network
SHA-256	Secure Hash Algorithm-256 (256 is the length of the digest)
SMS	Subscriber Management System
STKM	Short Term Key Message
TEK	Traffic Encryption Key
URI	Uniform Resource Identifier

References

ATSC

[ATSC-1] ATSC-Mobile DTV Standard

Part 2 – RF/Transmission System Characteristics: Document A/153 Part 2:2009, 15 October 2009

[ATSC-2] ATSC-Mobile DTV Standard

Part 3 – Service Multiplex and Transport Subsystem Characteristics:

Document A/153 Part 3:2009, 15 October 2009

[ATSC-3] ATSC-Mobile DTV Standard

Part 4 – Announcement : Document A/153 Part 4:2009, 15 October 2009

[ATSC-4] ATSC-Mobile DTV Standard

Part 6 – Service Protection : Document A/153 Part 6:2009, 15 October 2009

[ATSC-5] ATSC-ATSC Interaction Channel Protocols

Doc. A/96 : 3 February 2004

ETSI

[ESTSI-1] Digital Video Broadcasting (DVB)

DVB SimulCrypt;Head-end architecture and synchronization : ETSI TS 101 197

IETF

[IETF-1] Internet X.509 Public Key Infrastructure
Certificate and CRL Profile

http://www.ietf.org/rfc/rfc2459.txt

OMA

[OMA-1] OMA-DRM Specification V2.0

OMA-DRM-DRM-V2_0-20050426-C

[OMA-2] OMA-Service and Content Protection for Mobile Broadcast Services

OMA-TS-BCAST_SvcCntProtection-V1_0-20090212-A

[OMA-3] OMA-Service Guide for Mobile Broadcast Services

OMA-TS-BCAST_Service_Guide-V1_0-20090212-A

[OMA-4] OMA DRM v2.0 Extensions for Broadcast Support Approved Version 1.0

12 Feb 2009: OMA-TS-DRM_XBS-V1_0-20091212-A

OMVC

[OMVC-1] ATSC Mobile DTV Receiver Profile Guidelines V1.0

September 20, 2011 : http://www.omvc.org

PKI (Neustar)

[PKI-1] Mobile Digital Television (DTV) Certificate Policy

https://device.mobiledtvtrust.biz/cp.html

[PKI-2] Mobile Digital Television (DTV) Certificate Policy

https://rights.mobiledtvtrust.biz/cp.html