
# ATSC Mobile DTV Standard, Part 6 – Service Protection

Document A/153 Part 6:2011, 23 May 2011

**Advanced Television Systems Committee, Inc.**
1776 K Street, N.W., Suite 200
Washington, D.C. 20006

The Advanced Television Systems Committee, Inc., is an international, non-profit organization developing voluntary standards for digital television. The ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

Specifically, ATSC is working to coordinate television standards among different communications media focusing on digital television, interactive systems, and broadband multimedia communications. ATSC is also developing digital television implementation strategies and presenting educational seminars on the ATSC standards.

ATSC was formed in 1982 by the member organizations of the Joint Committee on InterSociety Coordination (JCIC): the Electronic Industries Association (EIA), the Institute of Electrical and Electronic Engineers (IEEE), the National Association of Broadcasters (NAB), the National Cable Telecommunications Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). Currently, there are approximately 140 members representing the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

ATSC Digital TV Standards include digital high definition television (HDTV), standard definition television (SDTV), data broadcasting, multichannel surround-sound audio, and satellite direct-to-home broadcasting. Contact information is given below.


| | |
|---|---|
| Mailing address | Advanced Television Systems Commmittee, Inc.<br>1776 K Street, N.W., Suite 200<br>Washington, D.C. 20006 |
| Telephone | 202-872-9160 (voice), 202-872-9161 (fax) |
| Web site | http://www.atsc.org, E-mail: standard@atsc.org |




The revision history of this document is given below.

A/153 Revision History

| | |
|---|---|
| A/153 approved | 15 October 2009 |
| Initial release of document | 28 November 2009 |
| Final publication | 12 February 2010 |
| 2011 revision approved | 23 May 2011 |

# Table of Contents

# Index of Tables and Figures

atsc
Advanced Television Systems Committee

# *ATSC Standard*: ATSC Mobile DTV Standard, Part 6 – Service Protection

## 1 SCOPE

The normative portions of this Part specify how Service Protection is to be encoded and signaled for ATSC Mobile DTV (mobile/handheld, or simply-M/H) broadcasts.

This Part makes direct references to functionality specified in the Open Mobile Alliance specifications for Service Protection (see reference [1]). Elements of those specifications which are not normatively referenced in this standard are not part of this standard, and are optional for ATSC-M/H broadcast Service Protection.

### 1.1 Organization

This document is organized as follows:

- **Section 1** – Outlines the scope of this Part and provides a general introduction.
- **Section 2** – Lists references and applicable documents.
- **Section 3** – Provides a definition of terms, acronyms, and abbreviations for this Part.
- **Section 4** – System overview and an introduction to Service Protection for ATSC-M/H.
- **Section 5** – Introduces the operational modes referred in this document.
- **Section 6** – OMA BCAST DRM Profile for Service Protection, organized to match those portions of reference [1] that are relevant to this application.
- **Section 7** – DRM extensions for broadcast support, organized to match those portions of reference [2] that are relevant to an OMA BCAST DRM Profile for Service Protection.
- **Section 8** – Describes the optional interactive mode of operation.
- **Section 9** – Describes the optional mixed-mode of operation.

This standard includes those portions of references [1] and [2] which are either required by the text in Section 6 and 7 below, or optional if so stated. Those portions of references [1] and [2] which are not referenced in this document are not included in the standard..

## 2 REFERENCES

At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this Part are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

### 2.1 Normative References

The following documents, in whole or in part, as referenced in this document, contain specific provisions that are to be followed strictly to implement provisions of this Part of this Standard.

[1] OMA: "Service and Content Protection for Mobile Broadcast Services," Open Mobile Alliance, OMA-TS-BCAST_SvcCntProtection-V1_0-20090212-A, available from http://www.openmobilealliance.org.

[2] OMA: "OMA DRM v2.0 Extensions for Broadcast Support," Open Mobile Alliance, OMA-TS-DRM_XBS-V1_0-20090212-A, available from http://www.openmobilealliance.org.

[3] IEEE: "Use of the International Systems of Units (SI): The Modern Metric System," Doc. IEEE/ASTM SI 10-2002, Institute of Electrical and Electronics Engineers, New York, N.Y.

### 2.2 Informative References

The following documents contain information that may be helpful in applying this Standard.

[4] ATSC: "ATSC Digital Television Standard, Part 2 – RF/Transmission System Characteristics," Doc. A/53 Part 2:2007, Advanced Television Systems Committee, Washington, D.C., 3 January 2007.

[5] ATSC: "ATSC Mobile/Handheld Digital Television Standard, Part 1 – Mobile/Handheld Digital Television System," Doc. A/153 Part 1:2009, Advanced Television Systems Committee, Washington, D.C., 15 October 2009.

[6] ETSI: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection," Doc. TS 102 474 V1.1.1 (2007-11).

[7] IEC: "Internet Protocol (IP) and Transport Stream (TS) Based Service Access," International Electrotechnical Commission, IEC 62455, First Edition, June 2007.

[8] FIPS: "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197.

[9] IETF: "IP Encapsulating Security Payload (ESP)," S. Kent, R. Atkinson, Doc. RFC 2406, Internet Engineering Task Force, Reston, VA, November 1998.

[10] ATSC: "ATSC Mobile/Handheld Digital Television Standard, Part 4 – Announcement," Doc. A/153 Part 4:2009, Advanced Television Systems Committee, Washington, D.C., 15 October 2009.

[11] ATSC: "ATSC Mobile/Handheld Digital Television Standard, Part 3 – Service Multiplex and Transport Subsystem Characteristics," Doc. A/153 Part 3:2009, Advanced Television Systems Committee, Washington, D.C., 15 October 2009.

[12] OMA: "Mobile Broadcast Services Architecture," Open Mobile Alliance, OMA-AD-BCAST-V1_0, available from http://www.openmobilealliance.org.

[13] OMA: "Mobile Broadcast Services Requirements," Open Mobile Alliance, OMA-RD-BCAST-V1_0, available from http://www.openmobilealliance.org.

[14] IETF: "Security Architecture for the Internet Protocol," Doc. RFC 2401, Internet Engineering Task Force, Reston, VA, November 1998.

## 3 DEFINITION OF TERMS

With respect to definition of terms, abbreviations, and units, the practice of the Institute of Electrical and Electronics Engineers (IEEE) as outlined in the Institute's published standards [3] shall be used. Where an abbreviation is not covered by IEEE practice or industry practice differs from IEEE practice, the abbreviation in question will be described in Section 3.3 of this document.

### 3.1 Compliance Notation

This section defines compliance terms for use by this document:

- **shall** – This word indicates specific provisions that are to be followed strictly (no deviation is permitted).
- **shall not** – This phrase indicates specific provisions that are absolutely prohibited.
- **should** – This word indicates that a certain course of action is preferred but not necessarily required.
- **should not** – This phrase means a certain possibility or course of action is undesirable but not prohibited.

### 3.2 Treatment of Syntactic Elements

This document contains symbolic references to syntactic elements used in the audio, video, and transport coding subsystems. These references are typographically distinguished by the use of a different font (e.g., restricted), may contain the underscore character (e.g., sequence_end_code) and may consist of character strings that are not English words (e.g., dynrng).

#### 3.2.1 Reserved Fields

**reserved** — The term "reserved", when used in the clauses defining the coded bit stream, indicates that the bit values are not defined and may be used in the future. Receiving devices are expected to disregard reserved bits, that is those for which no definition is available to that unit.

### 3.3 Acronyms and Abbreviation

The following acronyms and abbreviations are used within this Part.

**AES** – Advanced Encryption Standard

**BCRO** – Broadcast Rights Object

**BSD/A** – Broadcast Service Distribution/Adaptation Center

**BSM** – BCAST Subscription Management

**CTA** – Clear-to-Air

**DRM** – Digital Rights Management

**DVB** – Digital Video Broadcasting

**ID** – Identification

**FTA** – Free-to-Air

**IPsec** – IP Security

**LTKM** – Long-Term Key Message

**OMA** – Open Mobile Alliance

**PEK** – Program Encryption Key

**RI** – Rights Issuer

**RO** – Right Object

**ROT** – Root Of Trust

**SCR** – Static Conformance Requirements

**SEK** – Service Encryption Key

**SRTP** – Secure Real Time Protocol

**STKM** – Short-Term Key Message

**TEK** – Traffic Encryption Key

### 3.4 Terms

Definitions used in this document can be found in references [1] (OMA BCAST DRM Profile) and [2]. In addition, the following definitions are used in this document.

**Broadcast System** – The collection of equipment necessary to transmit signals of a specified nature, and support data exchange over the interaction channel.

**Clear-to-Air service** – A service that is sent unencrypted, and may be received via any suitable receiver with or without a subscription.

**Free-to-Air service** – A service that is sent encrypted, and for which the keys for decryption are available free of charge.

**IP stream** – A sequence of IP datagrams with the same source IP address and the same destination IP address.

**M/H Ensemble** – A collection of consecutive RS Frames with the same FEC coding, wherein each RS Frame encapsulates a specific number of data bytes arranged in datagrams.

**Reference Receiver** – A physical embodiment of hardware, operating system, and native applications of the manufacturer's choice, which collectively constitute a receiver for which specified transmissions are intended.

**Rights Issuer URI** – A string that identifies the Rights Issuer issuing RI Objects and Service Encryption Keys (SEKs). Rights Issuer URI type is anyURI.

**RI Object** – A binary coded Registration Layer message (see Section 7 of reference [2] (OMA DRM) or LTKM Layer message (see Section 8 of reference [2]). The term RI Object is defined to be an OMADRMBroadcastRightsObject with the message tag allocated in the Appendix C13 of reference [2].

**RI Stream** – A stream of UDP packets with the common source and destination IP addresses and UDP port, containing RI Objects.

**RS Frame** – Two-dimensional data frame by means of which the M/H Ensemble is RS CRC encoded. RS Frames are the output of M/H physical layer subsystem. Generally, one RS Frame contains 187 rows of N bytes each, where the value of N is determined by the transmission mode of M/H physical layer subsystem, and carries data for one M/H Ensemble. RS Frames are defined in detail in Part 2.

## 4 SYSTEM OVERVIEW

Please see ATSC A/153 Part 1 [5] for an overall description of the M/H system. The ATSC Mobile/Handheld service (M/H) shares the same RF channel as a standard ATSC broadcast

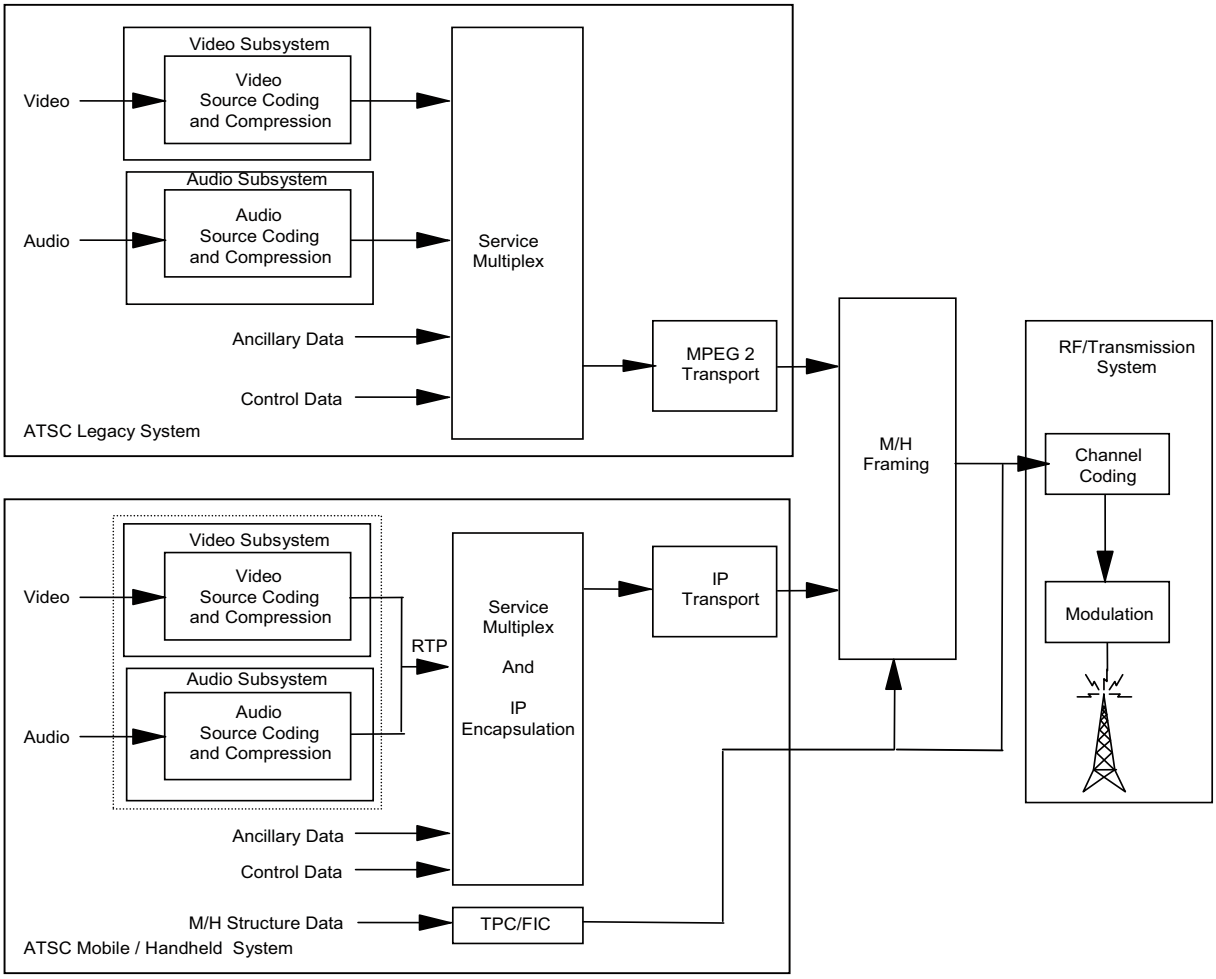


**Figure 4.1** ATSC broadcast system with TS Main and M/H services.

service described in ATSC A/53 [4]. M/H is enabled by using a portion of the total available ~19.4 Mbps bandwidth and utilizing delivery over IP transport. The overall ATSC broadcast system including standard (TS Main) and M/H systems is illustrated in Figure 4.1.

This Part details the Service Protection element of the ATSC-M/H broadcast service.

### 4.1 Service Protection Overview

The DRM based Service Protection profile has been introduced in three distinct specifications. The 18Crypt profile included in TS 102 474 [6], and the sections of reference [7] that deal with IP based service access, consist of a common set of features. OMA BCAST DRM Profile [1] adds new features, and the former are a backwards compatible subset of the OMA BCAST DRM Profile.

The ATSC-M/H Service Protection specified in this document is based on the OMA BCAST DRM Profile [1], and it uses features included in all three above mentioned specifications.

The ATSC-M/H Service Protection consists of the following components from reference [1]:

- Key provisioning as defined in Section 5.2 of reference [1].

- Layer 1 registration as defined in Section 5.3 of reference [1], excluding Broadcast Domains.
- Long-Term Key Message (LTKM) as specified in Section 5.4 of reference [1], including the use of Broadcast Rights Objects (BCROs) to deliver LTKMs, Sections 5.4.1 and 5.4.3 of reference [1].
- Short-Term Key Messages (STKM) as specified in Section 5.5 of reference [1].
- Traffic encryption as defined in Section 5.6 of reference [1]

The standard relies on the following encryption standards as detailed in Section 9 of reference [1]:

- Advanced Encryption Standard (AES), as specified in reference [8].
- Secure Internet Protocol (IPsec), as specified in reference [9].
- Traffic Encryption Key (TEK) as specified in reference [1].

### 4.2 Service Protection and Content Protection

Service Protection refers to the protection of content, be that files or streams, during its delivery to a receiver. Service Protection assumes no responsibility for content after it has been delivered to the receiver. It is intended for subscription management. It is an access control mechanism, only.

In this standard, Content Protection means protection of content subsequent to delivery through the service protection system. Content Protection deals with post-delivery usage rights.

In the OMA BCAST DRM Profile Service Protection, post-delivery usage rights can be communicated in Rights Objects (ROs) to a receiver. ROs may be delivered over an interaction channel or the broadcast channel. In case of the latter, Broadcast Rights Object (BCRO) messages are used.

This Part details the Service Protection for ATSC-M/H broadcast service, including the signaling of RO messages to a receiver. However, the Content Protection mechanism which uses the post-delivery usage rights is outside the scope of this Part.

### 4.3 Interactive Mode and Broadcast-Only Mode

In the OMA BCAST DRM Profile there are two modes for Service Protection-interactive and broadcast-only mode.

In interactive mode, the receiver supports an interaction channel to communicate with a service provider, to receive Service and/or Content Protection rights.

In broadcast-only mode, the receiver does not use an interaction channel to communicate with a service provider. Requests are made by the user through some out-of-band mechanism to the service provider, such as calling a service provider phone number or accessing the service provider website.

### 4.4 Overview of Operation

The OMA BCAST DRM Profile Service Protection solutions is based on a four-layer cryptographic architecture, with an optional optimization to provide both secure subscription and pay-per-view purchase options for a single service. Actual service encryption is carried out on the Traffic Encryption Layer according to AES [8] using 128 bit symmetric Traffic Encryption Keys (TEKs). This model is illustrated in Figure 4.2.

TEKs are applied following different mechanisms depending on the actual encryption protocol used.

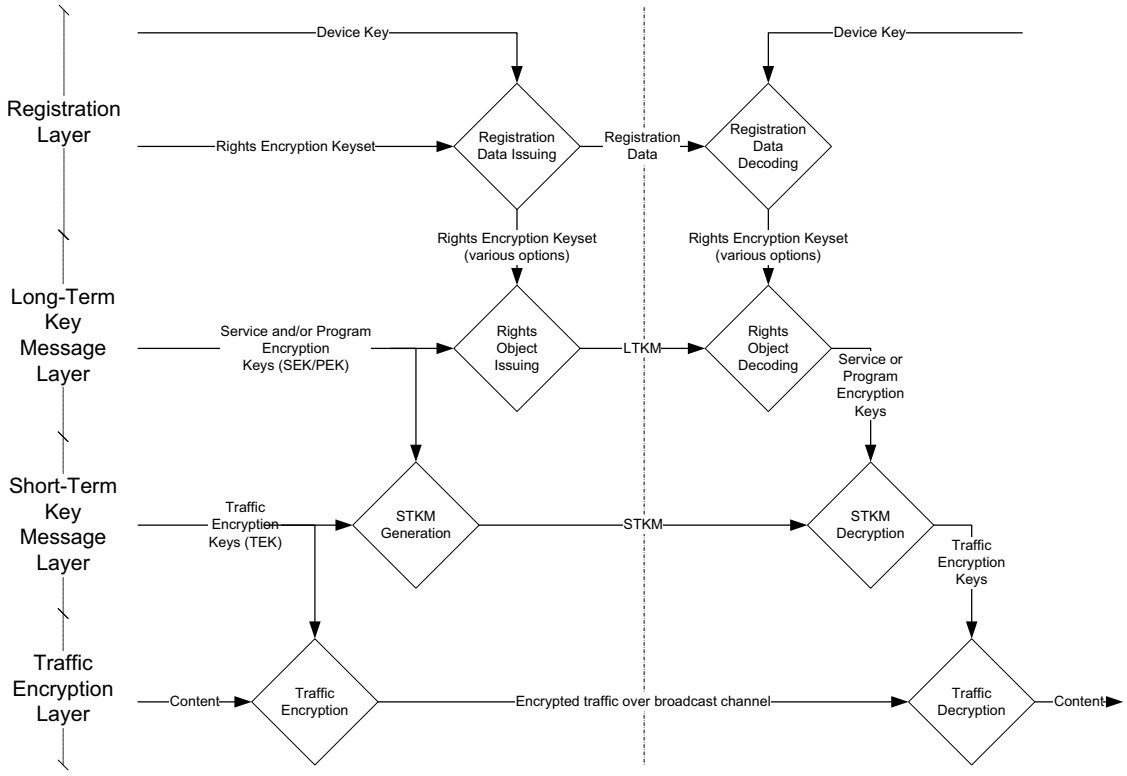


**Figure 4.2** Service Protection via the four-layer model.

The TEKs are protected with a Service Encryption Key (SEK) or Program Encryption Key (PEK) on the STKM layer, above the Traffic Encryption layer. The broadcast messages carrying TEKs are called Short Term Key Messages (STKMs).

STKMs can contain two levels of encryption. Separate Program and Service Encryption Keys have different lifetimes and can be used to provide, for a single service, different granularities of purchase periods to different users. This allows for the efficient implementation of both subscription and pay-per-view business models for the same service. Pay-per-view customers are provided with a Program Encryption Key (PEK) which is only valid for a single program while subscribers are given a Service Encryption Key (SEK), valid for reception of the service for some longer period. Within the STKM, the TEK is encrypted with a PEK, and the PEK is also carried, encrypted with the SEK. Thus, pay-per-view subscribers can directly decrypt the TEK, while subscribers can decrypt the PEK using the SEK, which can then be used to decrypt the TEK.

STKMs contain extensions to content IDs, which are carried in the Announcement (see A/153 Part 4 [10]) or Signaling (see A/153 Part 3 [11]), for the program and/or service. Receivers use this ID to identify which Rights Object contains the keys to use for STKM decryption.

Where the two-level service and program functionality is not required (i.e., when subscription and pay-per-view purchase options are not required simultaneously for a single service) the TEK can be directly encrypted with either the SEK or PEK and the SEK-encrypted PEK omitted.

The SEK(s) or PEK(s) are delivered to receivers within Rights Objects (ROs). Such delivery of ROs can be done via a broadcast channel (broadcast-only mode), or by using the separate

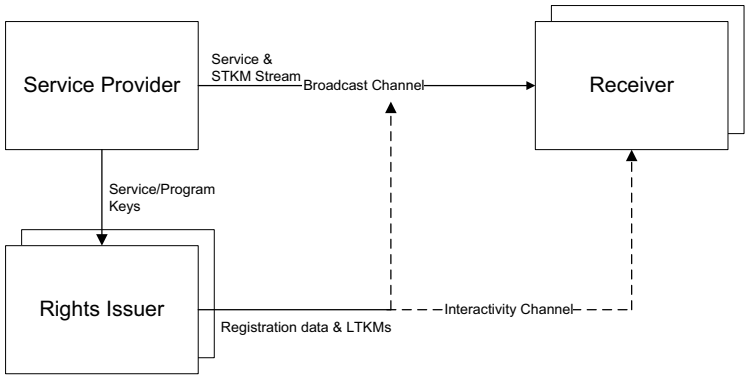


**Figure 4.3** Highly simplified view of the end-to-end system.

interaction channel (interactive mode). In both cases the ROs can be utilized by the customer receivers only.

When delivering Rights Objects over the broadcast channel, bandwidth is a major constraint. In OMA BCAST DRM Profile, this problem is addressed in two complementary ways. Firstly, a binary form of the Rights Object, called a Broadcast Rights Object (BCRO), is defined. Secondly, a method is described for securely delivering BCROs to groups of receivers using a single broadcast message. Valuable portions of Rights Objects are protected by group or unit keys, and when necessary, Zero Message Broadcast encryption can be used to allow messages to be decrypted only by arbitrary sets of receivers within a larger group.

### 4.5 The End-to-End System

This section briefly describes the major roles within the OMA BCAST DRM Profile Service Protection system. Figure 4.3 shows a simplified view of the major actors in the system and their relationship to each other. The main actors are as follows:

- The Service Provider broadcasts and encrypts the service and the key stream. It provides Service and Program keys to the Rights Issuers.
- The Rights Issuer registers receivers as subscribers to the services and provides Rights Objects to those receivers allowing them to decrypt the services which they are entitled to receive.
- The receiver receives the service, decrypts it (assuming it has the necessary Rights Objects) and presents it to the user.

## 5 SERVICE PROTECTION OPERATIONAL MODES

It is optional for an ATSC-M/H service to utilize Service Protection. When Service Protection is used, the ATSC M/H emission shall conform to the provisions of this Part.

The Service Protection support in Broadcast Systems and the Reference Receiver shall conform with the OMA BCAST DRM Profile, specified in references [1] and [2], with the adjustments specified in this Part.

OMA BCAST DRM Profile specifies three operational modes-broadcast-only mode, interactive mode, and mixed-mode. Broadcast Systems shall support the broadcast-only mode, the interactive mode and mixed-mode. The Reference Receiver shall support the broadcast-only

mode, the interactive mode (when an interaction channel is instantiated) and the mixed-mode (when an interaction channel is instantiated).

The periods between transmissions either of LTKMs or of STKMs shall not exceed, but may be equal to, the lifetimes of the keys carried within the respective message types.

# 6 OMA BCAST DRM PROFILE FOR ATSC-M/H SERVICE PROTECTION (BROADCAST-ONLY MODE)

This Part defines Service Protection for ATSC-M/H content based upon an OMA BCAST DRM Profile, as given in reference [1].

Any normative requirements in this document apply only to ATSC-M/H Broadcast Systems and the Reference Receiver that support Service Protection.

## 6.1 Selected Features

The following is a non-exclusive list of mandatory features in this Part. Further details of each feature are given in later sections. Reference pointers are given in Table 6.1.

**Table 6.1** Feature Reference Pointers

| Feature | Reference |
|---|---|
| OMA BCAST DRM Profile for Service Protection | |
| Broadcast-only mode | Section 5.2.1 of [2] |
| Authentication of Traffic Layer, Key Stream Layer and Rights Management Layer | Section 6 of [2] |
| Broadcast Device Registration | Section 7.2. of [2] |
| Inform Registered Device Protocol | Section 7.5 of [2] |
| Forced re-registration | Section 7.5.2 of [2] |
| Update RI Certificate | Section 7.5.3 of [2] |
| Update DRM Time | Section 7.5.4 of [2] |
| Binary coded RO (BCRO) over broadcast channel | Sections 8.1 and 8.2 of [2] |
| Access permission | Section 8.4.2 of [2] |
| LTKM signaling on SDP | Section 10.1.4 of [1] |
| Fixed Subscriber Groups | Section 10.3.3.1 of [2] |
| Zero-Message Broadcast Encryption | Section 10.3.4.4 of [2] |
| Right Issuer Services | Section 12 of [2] |
| IPsec | Section 9.1 of [1] |
| STKM for DRM Profile | Section 5.5 of [1] |
| STKM signaling on SDP | Section 10.1.2 of [1] |

## 6.2 Streaming and Content Download Using Service Protection

Support for streaming using Service Protection shall conform with specifications in Sections 4.1.2.1 and 4.1.2.2 of OMA BCAST DRM Profile [1], using IPsec. Support for content download using Service Protection shall conform to Section 4.1.3 (including sub-sections) of reference [1], using IPsec.

There are two defined options for filtering encrypted and clear packets of a multicast component stream of a given destination IP address:

- "Option A" permits filtered encryption, resulting in only some of the packets of a multicast component stream of a given destination IP address being encrypted. For example, should RTP and RTCP packets be carried on a common destination IP address and on different UDP port, RTP could be encrypted while RTCP may be in the clear. Option A allows that, for example, an IPSec security policy with a UDP port selector is used for unencrypted traffic with a BYPASS (no protection) action; e.g., UDP port selector for the port which carries the RTCP traffic. See Section 4.4.1.1 of RFC 2401 [14] for more information on selectors.
- "Option B" constrains the encryption such that if any packet of a multicast component stream of a given destination IP address are encrypted, then all the packets of the stream shall be encrypted (i.e., there is no encryption filtering, for example on UDP ports).

For signaling of which option is used, see the MH_service_protection_filtering_option in the protection_descriptor used in the Service Map Table in Section 7.8.11 of A/153 Part 3 [11].

### 6.3 Long-Term Key Message

The Long-Term Key Messages shall conform with specifications in Section 5.4 (including sub-sections) of OMA BCAST DRM Profile [1], with the following constraints:

- LTKM shall contain Access permission to allow immediate rendering of the content, and may contain an Export permission with system constraint "urn:oma:drms:org-cmla:plaintext" to allow exporting in clear format.

  Note that the future versions of ATSC-M/H may change this constraint. Receiver implementations shall not expect the presence of any particular permission, but shall verify the presence in corresponding LTKM.

### 6.4 Short-Term Key Message

The Short-Term Key Messages shall be constructed and sent as described in Sections 5.5 and 7 (including sub-clauses) of OMA BCAST DRM Profile [1], with the following constraints:

- protection_after_reception shall be set to 0, and permission_category, if present, shall be set to 0xFF (no post-acquisition content protection; export in plaintext is allowed).

  Note that the future versions of ATSC-M/H may allow other values for the permission_category. Receiver implementations shall respect the concerned post-acquisition rules. For example, a receiver may decide not to decrypt services where permission_category is set to any other value but 0xFF.

- traffic_protection_protocol shall be set to TKM_ALGO_IPSEC (IPsec ESP used).
- Parental rating information, if contained in an STKM, shall have no meaning.
- Implementations may support descriptors specified in Section 7.1 of reference [1].
- If a protected component is associated with multiple STKM Streams issued by different Rights Issuers, Signaling (A/153 Part 3) [11] shall provide the relevant Rights Issuer URIs for each of the STKM Streams.

### 6.5 Encryption Protocols

The Reference Receiver shall support IPsec.

The encryption protocols shall be used as defined in Section 9 (and sub-clauses) of OMA BCAST DRM Profile [1].

Use of traffic encryption protocols not referred in the Section 9 (including sub-sections) of reference [1] are explicitly outside the scope of this Part.

### 6.6 Signaling

The signaling of protected services and associated key streams shall conform with specifications in Section 10 (and sub-clauses) of reference [1].

### 6.7 Common Keys / Sharing Streams for DRM Profile and Smartcard Profile

Support for specifications in Section 11 (and sub-clauses) of [1] is not in the scope of this Part.

### 6.8 Conversion Between Time and Date Conventions

The coding of the STKM timestamp field, when present, shall be as specified in Section 14 (and sub-clauses) of reference [1].

### 6.9 Static Conformance Requirements

Broadcast Systems and the Reference Receiver systems shall conform with the SCR in Appendix B of reference [1], with the adjustments specified in this Part.

The following is a non-exclusive list of adjustments on the SCR in reference [1]:

- BCAST mandatory items, not mandatory in the context of this Part:
  1) SCR for Clients (Section B.1 of reference [1]):
     a) Reference Receiver support for Smartcard Profile is explicitly outside the scope of this Part. Changes requirements of item BCAST-TerminalCapability-C-003 (reference to BCAST-SPCP-C-005).
     b) Reference Receiver support for SRTP is optional. Changes requirements of item BCAST-SPCP-C-006 (reference to BCAST-ContentLayer-C-007).
  2) SCR for BSD/A (Section B.2 of reference [1]):
     a) Broadcast System support for backend interfaces is optional. Changes requirements of item BCAST-BSDASPCP-S-001 (references to BCAST-BSDASPCP-S-002 and BCAST-BSDASPCP-S-003) and item BCAST-BSDASPCP-S-004 (reference to BCAST-BSDASPCP-S-005).
     b) Broadcast System support for Service Protection of Streams is optional. Changes requirements of item BCAST-BSDASPCP-S-007 (reference to BCAST-BSDASPCP-S-009).
     c) Broadcast System support for Service Protection of files is optional. Changes requirements of item BCAST-BSDASPCP-S-007 (reference to BCAST-BSDASPCP-S-010).
  3) SCR for BSM (Section B.3 of reference [1]):
     a) Broadcast System support for backend interfaces is optional. Changes requirements of item BCAST-BSMSPCP-S-001 (references to BCAST-BSMSPCP-S-002 and BCAST-BSMSPCP-S-003) and item BCAST-BSMSPCP-S-004 (reference to BCAST-BSMSPCP-S-005).
- BCAST optional items, mandatory in the context of this Part:
  1) SCR for Clients (Section B.1 of reference [1]):

a) Reference Receiver support for IPsec is mandatory. Changes requirements of item BCAST-SPCP-C-006 (reference to BCAST-ContentLayer-C-008).

# 7 DRM EXTENSIONS FOR BROADCAST SUPPORT (BROADCAST-ONLY MODE)

This section defines service key messaging extensions for broadcast support as given in reference [2].

## 7.1 Four-Layer Key Hierarchy for Service Protection

The key hierarchy shall conform with specifications in Section 5 (including sub-section) of OMA DRM v2.0 Extensions [2].

The Reference Receiver shall support the use of SEK (Service Encryption Key).

The Reference Receiver may support the use of PEK (Program Encryption Key). Note that if a receiver does not support the use of PEK, it might not be able to decrypt a program protected using a PEK. However, if the program is protected using both PEK and SEK, the receiver could subscribe the SEK and therefore become able to decrypt the program.

### 7.1.1 Registration Layer – Layer 1 Keys (Broadcast Mode)

Registration Layer shall conform with specifications in Section 5.1 of reference [2].

### 7.1.2 Long-Term Key Message Layer – Layer 2 Keys

In broadcast-only mode, LTKM Layer shall conform with specifications in Section 5.2.1 of reference [2].

### 7.1.3 Short-Term Key Message Layer – Layer 3 Keys

STKM Layer shall conform with specifications in Section 5.3 (including sub-sections) of reference [2].

### 7.1.4 Traffic Encryption Layer – Layer 4 Keys

Traffic Encryption Layer shall conform with specifications in Section 5.4 of reference [2].

## 7.2 Authentication

Authentication shall conform with what is specified in Section 6 (including sub-sections) of reference [2].

## 7.3 Broadcast Device and Domain Management

Broadcast Systems and the Reference Receiver shall conform with specifications in Section 7 (including sub-sections) of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

Encoding, format and protocol for the data delivered from the Reference Receiver to the Broadcast System as specified in Section 7 (including sub-sections) of the reference [2] may be supported.

Specifications in Section 7.4 (including sub-sections) of reference [2] may be supported. Other methods, such as web-portal, for offline-notification may be used, depending on the actual commercial adoption.

Following adaptations apply to Broadcast Systems and the Reference Receiver:

- device_registration_response message specified in Section 7.2.2 (including sub-sections) of reference [2] shall be supported.
- Encoding, format and protocol for the data delivered from the Broadcast System to the Reference Receiver shall conform with specifications in Section 7 (including sub-sections) of reference [2].
- The Reference Receiver shall have a globally unique UDN (Unique Device Number) as specified in Section 7.2.1.2 of reference [2].
- Forced re-registering as specified in Section 7.5.2 (including sub-sections) of reference [2] shall be supported. When receiving the re_register_msg, the receiver should enter into registration mode. The Reference Receiver may consult the user before entering the registration mode. The re-registration message shall contain status field in between longform_udn and the signature_type_flag, as specified in Section 7.5.2.1.1 of reference [2]. The field shall be 8 bits.
- Update RI Certificate as specified in Section 7.5.3 (including sub-sections) of reference [2] shall be supported.
- Update DRM Time as specified in Section 7.5.4 (including sub-sections) of reference [2] shall be supported.
- Update Contact Number as specified in Section 7.5.5 (including sub-sections) of reference [2] may be supported.
- Tokens may be supported. If tokens are supported, the support shall conform with specifications in Section 7.6 (including sub-sections) of reference [2].
- Domains may be supported. If domains are supported, the support shall conform with specifications in Section 7.7 (including sub-sections) of reference [2].

## 7.4 Broadcast Rights

The broadcast delivery of LTKMs shall conform with specifications in Sections 8.1 (including sub-sections) and 8.2 (including sub-sections) of OMA DRM v2.0 Extensions [2].

Broadcast Systems and the Reference Receiver shall support at least the following addressing modes (other addressing modes may be supported):

- 0x0 a whole Fixed Subscriber Group
- 0x1 subgroup of a Fixed Subscriber Group
- 0x2 a unique receiver

### 7.4.1 Access Permission

The Reference Receiver shall support the access permission. For more on access permission, see Sections 8.2.6 and 8.4.2 of reference [2].

## 7.5 Token Management

Broadcast Systems and the Reference Receiver may support tokens. If tokens are supported, the support shall conform with specifications in Section 9 (including sub-sections) of OMA DRM v2.0 Extensions [2].

### 7.6 Subscriber Groups

Broadcast Systems and the Reference Receiver shall support Subscriber Groups as specified in Section 10 (including sub-sections) of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

Fixed Subscriber Groups shall be supported.

### 7.7 Broadcast Service Support

Key Stream handling shall conform with specifications in Section 11 (including sub-sections) of OMA DRM v2.0 Extensions [2].

### 7.8 RI Object delivery

Delivery of RI Objects over broadcast channel shall conform with the specifications in Section 12 (including sub-sections) of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

#### 7.8.1 RI Stream

RI Stream packet format shall conform with the specifications in Section 12.5.2 of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

RI Stream shall not contain any other objects or messages but RI Objects.

Any service may have any number of RI Stream components. An RI Stream may be a component of multiple services simultaneously.

##### 7.8.1.1 In-band RI Stream

An RI Stream component of any other service but Rights Issuer Service is an In-band RI Stream. A Rights Issuer may provide In-band RI Streams. In-band RI Stream shall conform with specifications in Section 12.4 of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

Signaling (A/153 Part 3) [11] shall associate each In-band RI Stream with exactly one Rights Issuer URI, which identifies the Rights Issuer issuing the RI Stream. A service shall not have multiple In-band RI Streams associated with the same Rights Issuer URI.

When receiving a protected service which has In-band RI Stream components, a receiver is expected to listen to the In-band RI Stream for each Rights Issuer which it is registered, as specified in the Section 12.4 of OMA DRM v2.0 Extensions [2].

##### 7.8.1.2 Ad-hoc RI Stream

An RI Stream that carries device_registration_response messages is an Ad-hoc RI Stream. Ad-hoc RI Stream shall conform with specifications in Section 12.3 of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

- Ad-hoc RI Stream shall be a component of a Rights Issuer Service.
- Ad-hoc RI Stream may contain any RI Objects.
- Ad-hoc RI Stream component shall not be encrypted.

#### 7.8.2 Rights Issuer Service

Rights Issuer Service is a service which has only RI Stream components, and optionally one FLUTE file delivery session channel. Rights Issuer Service shall conform with specifications in

Section 12 (including sub-sections) of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

For each Rights Issuer Service, Signaling (A/153 Part 3) [11] shall associate exactly one Rights Issuer URI, which identifies the Rights Issuer issuing the RI Stream components of the service. An M/H Ensemble shall not have multiple Rights Issuer Services associated with a given Rights Issuer URI.

Rights Issuer Service may have multiple RI Stream components, and may have up to one FLUTE file delivery session component, and shall not have other components.

#### 7.8.2.1 FLUTE File Delivery Session Component

Rights Issuer Service may provide schedule for RI Object transmission. Schedule shall conform with specifications in Section 12.7 (including sub-sections) of OMA DRM v2.0 Extensions [2], with the adjustments specified in this document.

When provided, schedule shall be provided in the FLUTE file delivery session component of the actual Rights Issuer Service.

The component shall not be encrypted.

The component shall contain one or more RightsIssuerServiceData files specified in Section 12.7.1 of reference [2]. The files may be compressed with the GZIP algorithm. When GZIP compression is used, the corresponding 'Content-Encoding' attributes shall be set to "gzip".

In each file, the ipAddress and port attributes of the RightsIssuerStream element in the Rights Issuer Service Data structure, if provided, shall refer to an RI Stream component of the actual Rights Issuer Service. In other words, schedule shall be provided only for RI Stream components of the actual Rights Issuer Service, and shall not be provided for any RI Stream that is not a component of the actual Rights Issuer Service.

Broadcast Systems may deviate from the schedule. Note that this might cause registered receivers to miss delivered RI Objects.

#### 7.8.2.2 RI Stream Components

Any Ad-hoc RI Stream component of a Rights Issuer Service shall be identified in Signaling (A/153 Part 3) [11]. A receiver is expected to listen to all Ad-hoc RI Stream components of a Rights Issuer Service when listening to any of the components of the service.

If schedule is not provided, a registered receiver is expected to periodically listen to all components of the service, as specified in the Section 12.11 of the OMA DRM v2.0 Extensions [2].

If schedule is provided, a registered receiver may expect the schedule applies for all RI Stream components of the service, excluding any Ad-hoc RI Stream components. In other words, the receiver may decide to listen to the Rights Issuer Service only at the scheduled times, as explained in Section 12.2 of reference [2]. In such case, the receiver may decide to listen to only the FLUTE file delivery session component, all Ad-hoc RI Stream components and the scheduled RI Stream component.

### 7.9 Static Conformance Requirements

Broadcast Systems and the Reference Receiver shall conform with the SCR in Appendix B of reference [2], with the adjustments specified in this document.

Following is a non-exclusive list of adjustments on the SCR in OMA DRM v2.0 Extensions [2]:

- BCAST mandatory items, not mandatory in the context of this Part:
  1) SCR for XBS Clients (Section B.1 of reference [2]);
     a) Reference Receiver support for Offline-Notification of Short Device Data is optional. Changes requirements of item BCAST-XBS-C-008 (reference to BCAST-XBS-C-010).
     b) Reference Receiver support for Update Contact Number is optional. Changes requirements of item BCAST-XBS-C-013 (reference to BCAST-XBS-C-016).
     c) Reference Receiver support for tokens is optional. Changes requirements of item BCAST-XBS-C-003 (references to BCAST-XBS-C-053 and BCAST-XBS-C-054).
     d) Reference Receiver support for domains is optional. Changes requirements of item BCAST-XBS-C-003 (reference to BCAST-XBS-C-019).
  2) SCR for XBS Servers (Section B.2 of reference [2]);
     a) Broadcast System support for tokens is optional. Changes requirements of item BCAST-XBS-S-003 (references to BCAST-XBS-S-018 and DRM-XBS-S-053).
     b) Broadcast System support for Offline-Notification of Short Device Data is optional. Changes requirements of item BCAST-XBS-S-008 (reference to DRM-XBS-S-010).
     c) Broadcast System support for Update Contact Number is optional. Changes requirements of item BCAST-XBS-S-013 (reference to BCAST-XBS-S-017).
     d) Broadcast System support for domains is optional. Changes requirements of item BCAST-XBS-S-003 (reference to BCAST-XBS-S-019).
- BCAST optional items, mandatory in the context of this Part:
  1) SCR for XBS Clients (Section B.1 of reference [2]);
     a) Reference Receiver support for Fixed Subscriber Groups is mandatory. Changes requirements of item BCAST-XBS-C-029 (reference to BCAST-XBS-C-030).
     2) SCR for XBS Servers (Section B.2 of reference [2]);
     a) Server support for Fixed Subscriber Groups is mandatory. Changes requirements of item BCAST-XBS-S-029 (reference to BCAST-XBS-S-030).

### 7.10 Message Tags

Broadcast Systems and the Reference Receiver shall support at least the following message tags listed in Section C.13 of OMA DRM v2.0 Extensions [2] (other message tags may be supported):

- 0x01 device_registration_response
- 0x11 re_register_msg
- 0x12 update_ri_certificate_msg
- 0x13 update_drmtime_msg
- 0x20 OMADRMBroadcastRightsObject

# 8 OMA BCAST DRM PROFILE FOR ATSC-M/H SERVICE PROTECTION (INTERACTIVE MODE)

This section describes the implementation of interactive mode for ATSC-M/H devices. Broadcast Systems and Reference Receivers (with an interaction channel instantiated) shall support interactive mode as specified below.

## 8.1 Selected Features

The following is a non-exclusive list of mandatory features when interactive mode is supported. Further details of each feature are given in later sections. Reference pointers are given in Table 8.1..

**Table 8.1** Feature Reference Pointers

| Feature | Reference |
|---|---|
| On-line registration | Section 7.3 of [2] |
| Acquisition of Rights Objects over an Interaction Channel | Section 8.3 of [2] |
| Access permission | Section 8.4.2 of [2] |

## 8.2 On-Line Registration

The Reference Receiver and Broadcast System supporting interactive mode shall register as specified for interactive device in Section 7.3 of OMA DRM v2.0 Extensions [2].

## 8.3 Acquisition of Rights Objects over an Interaction Channel

The Reference Receiver and Broadcast System supporting interactive mode shall support acquisition of Rights Objects over an interaction channel as specified in Section 8.3 of OMA DRM v2.0 Extensions [2].

## 8.4 Access Permission

The Reference Receiver and Broadcast System supporting interactive mode shall support acquisition the access permission as specified in Section 8.4.2 of OMA DRM v2.0 Extensions [2].

## 8.5 Static Conformance Requirements

The Reference Receiver and Broadcast Systems that support interactive mode shall conform with the SCR adjustments defined above for broadcast-mode devices (SCR in Appendix B of OMA DRM v2.0 Extensions [2]), with the following additions.

Following is a non-exclusive list of adjustments on the SCR in reference [2]:

BCAST mandatory items, not mandatory in the context of this Part:

SCR for XBS Servers (Section B.2 of reference [2]);

Broadcast System support for tokens is optional. Changes requirements of item BCAST-XBS-S-002 (reference to DRM-XBS-S-028).

# 9 OMA BCAST DRM PROFILE FOR ATSC-M/H SERVICE PROTECTION (MIXED-MODE)

This section describes the implementation of mixed mode for ATSC-M/H devices. Broadcast Systems and Reference Receivers (with an interaction channel instantiated) shall support mixed-mode, as specified below.

### 9.1 Selected Features

The following is a non-exclusive list of mandatory features when mixed-mode is supported. Further details of each feature are given in later sections. Reference pointers are given in Table 9.1.

**Table 9.1** Feature Reference Pointers

| Feature | Reference |
|---|---|
| On-line registration | Section 7.3 of [2] |
| Acquisition of Rights Objects over an Interaction Channel | Section 8.3 of [2] |
| Access permission | Section 8.4.2 of [2] |

### 9.2 On-Line Registration

The Reference Receiver and Broadcast Systems supporting mixed-mode shall register as specified for mixed-mode in Section 7.3 (including sub-sections) of OMA DRM v2.0 Extensions [2]. ROAP registration extensions shall be used as specified in Sections 7.3.1 and 7.3.2 (including sub-sections) of reference [2].

### 9.3 Acquisition of Rights Objects over an Interaction Channel

The Reference Receiver and Broadcast Systems supporting mixed-mode shall support acquisition of Rights Objects over an interaction channel as specified in Section 8.3 of OMA DRM v2.0 Extensions [2].

For a communication initiated by a mixed-mode Reference Receiver over the interaction channel, the corresponding Broadcast System shall respond over the same channel. Any communication initiated from the Broadcast System to a mixed-mode Reference Receiver shall be delivered over the broadcast channel.

### 9.4 Access Permission

The Reference Receiver and Broadcast Systems supporting mixed-mode shall support acquisition the access permission as specified in Section 8.4.2 of OMA DRM v2.0 Extensions [2].

### 9.5 Static Conformance Requirements

The Reference Receiver and Broadcast Systems that support mixed-mode shall conform with the SCR adjustments defined above for broadcast-mode devices (SCR in Appendix B of OMA DRM v2.0 Extensions [2]), with the following additions.

Following is a non-exclusive list of adjustments on the SCR in reference [2]:

BCAST mandatory items, not mandatory in the context of this Part:

SCR for XBS Servers (Section B.2 of reference [2]);

Broadcast System support for tokens is optional. Changes requirements of item BCAST-XBS-S-002 (reference to DRM-XBS-S-028).

atsc
Advanced Television Systems Committee


**Advanced Television Systems Committee, Inc.**
1776 K Street, N.W., Suite 200
Washington, D.C. 20006