ATSC Standard: Conditional Access System for Terrestrial Broadcast Service Protection using Simulcrypt for Internet Protocol-Delivered Services

Doc. A/70 Part 2:2011
17 October 2011

Advanced Television Systems Committee
1776 K Street, N.W., Suite 200
Washington, D.C. 20006
202-872-9160

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 Television 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.

Note: The user's attention is called to the possibility that compliance with this Standard may require use of an invention covered by patent rights. By publication of this Standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. One or more patent holders have, however, filed a statement regarding the terms on which such patent holder(s) may be willing to grant a license under these rights to individuals or entities desiring to obtain such a license. Details may be obtained from the ATSC Secretary and the patent holder.

Table of Contents

1. SCOPE 4
1.1 Introduction and Background 4
1.2 Organization 4
2. REFERENCES 4
2.1 Normative References 4
2.2 Informative References 5
3. DEFINITION OF TERMS 5
3.1 Compliance Notation 5
3.2 Treatment of Syntactic Elements 5
3.2.1 Reserved Elements 5
3.3 Acronyms and Abbreviation 6
3.4 Terms 6
4. ATSC SERVICE PROTECTION WITH SIMULCRYPT 6
4.1 Multiplexer and Scrambler Interfaces 6
4.2 Conditional Access System and Operator Identification 6
4.3 EMM Transport 6
4.4 ECM Transport 6
4.5 Scrambling Control Word Updates (informative) 7
5. SIGNALING IN A/153 SYSTEMS 7
5.1 Conditional Access System Identification Fields 7
5.2 EMM Streams 7
5.2.1 EMM Streams Signaling 7
5.2.2 EMM Streams Announcement Signaling 8
5.3 ECM Streams 8
5.3.1 ECM Stream Signaling 8
5.3.2 ECM Streams Announcement Signaling 9

Index of Tables

Table 5.1 Conditional Access System and Operator Identification Fields 7
Table 5.2 Bit Stream Syntax for M/H Component Data for Service Protection Identification (Type 0x43) 8
Table 5.3 Bit Stream Syntax for M/H Component Data for ECM Identification (Type 0x44) 9

ATSC Standard: Conditional Access System for Terrestrial Broadcast Service Protection using Simulcrypt for Internet Protocol-Delivered Services A/70 Part 2

1. SCOPE

Part 2 of this Standard defines the method for utilizing Simulcrypt concepts to simultaneously encrypt (provide service protection) services with different service protection systems without transmitting multiple differently-encrypted copies of the services.

1.1 Introduction and Background

Part 2 of this Standard describes an architecture that is applicable to terrestrial (over-the-air) broadcast systems delivered upon an IP delivery framework.

This Standard may be applied to the broadcast of ATSC Mobile DTV signals and services and other IP-delivered services, and allows broadcasters to field pay services using alternate service protection systems.

1.2 Organization

This document is organized as follows:

- **Section 1** – Outlines the scope of this document and provides a general introduction
- **Section 2** – Lists references and applicable documents
- **Section 3** – Provides a definition of terms, acronyms, and abbreviations for this document
- **Section 4** – System specifications (normative)

2. REFERENCES

At the time of publication, the editions indicated were valid. All referenced documents are subject to revision, and users of this Standard are encouraged to investigate the possibility of applying the most recent edition of the referenced document.

2.1 Normative References

The following documents, in whole or in part, as referenced in this document, contain provisions that are necessary to implement a mandatory or optional provision of this Standard.

[1] 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] 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.

[3] 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.

[4] OMA: "Service Guide for Mobile Broadcast Services," Open Mobile Alliance, OMA-TS-BCAST_Service_Guide-V1_0, available from http://www.openmobilealliance.org.

[5] ETSI: "IP Datacast over DVB-H: Content Delivery Protocol," Doc. ETSI TS 102 472 – v1.3.1.

[6] ISO/IEC: "Information Technology — Generic coding of moving pictures and associated audio — Part 1: systems,", Doc. ISO/IEC 13818-1:2007. Available from the International Telecommunications Union at www.itu.org (as ITU-T Rec. H.222.0), and Global Engineering Documents at www.global.ihs.com.

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

2.2 Informative References

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

[8] ETSI: "Head-end implementation of DVB SimulCrypt" Doc. ETSI TS 103 197 – V1.5.1, November, 2006.

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 [1] 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

As used in this document, "shall" denotes a mandatory provision of the standard. "Should" denotes a provision that is recommended but not mandatory. "May" denotes a feature whose presence does not preclude compliance, which may or may not be present at the option of the implementer.

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 Elements

One or more reserved bits, symbols, fields, or ranges of values (elements) may be present in this document. These are primarily used to enable adding new values to a syntactical structure without altering the syntax or causing a backwards compatibility issue, but also are used for other reasons.

The ATSC default value for reserved bits is '1.' There is no default value for other reserved elements. Use of Reserved elements except as defined in ATSC Standards or by an industry standards setting body is not permitted. See individual element semantics for mandatory settings and any additional use constraints. As reserved elements may be changed in subsequent version(s) of the Standard, receiving devices are expected to disregard reserved elements independent of the defined value for that element.

3.3 Acronyms and Abbreviation

The following acronyms and abbreviations are used within this specification.

ATSC – Advanced Television Systems Committee

bslbf – bit serial, leftmost bit first

ECM – Entitlement Control Message, in OMA BCAST DRM terms, the STKM

EMM – Entitlement Management Message, in OMA BCAST DRM terms, the LTKM

KMS – Key Management System, a component of a Conditional Access System

TEK – Traffic Encryption Key

uimsbf – unsigned integer, most significant bit first

3.4 Terms

The following terms are used within this specification.

encryption – The method of protecting EMM and ECM messages by cryptographic methods.

host – A device where module(s) can be connected. For example, a television, an integrated receiver-decoder, or a PC.

module – A small device, not working by itself, designed to run specialized conditional access processing in association with a host. For example, a conditional access subsystem.

reserved – An element that is set aside for use by a future Standard.

scrambling – The method of obscuring digital streams by cryptographic methods.

4. ATSC SERVICE PROTECTION WITH SIMULCRYPT

4.1 Multiplexer and Scrambler Interfaces

This Standard does not specify or define multiplexer or scrambler interfaces. However, to maximize interoperability and to support multiple CA vendors, it is recommended that these interfaces comply with the Head-end Implementation of DVB Simulcrypt [8], particularly Annex N.

4.2 Conditional Access System and Operator Identification

Simulcrypt key streams (EMM and ECM streams) are associated with specific conditional access systems and system operators. Signaling of the Conditional Access System and Operator Identification depends on the system information in use. For ATSC A/153 systems, this mechanism is described in Section 5.

4.3 EMM Transport

The EMMs shall be transported as User Datagram Protocol (UDP)/IP packets. Each packet may contain any number of complete EMMs. EMMs are carried in the payload without any additional packetization or signaling.

4.4 ECM Transport

The ECMs shall be transported as UDP/IP packets. Each packet may contain any number of complete ECMs. ECMs are carried in the payload without any additional packetization or signaling.

4.5 Scrambling Control Word Updates (informative)

When IPsec is used, key change signaling at the IP level is needed. Each IPSec packet header includes the Security Parameter Index (SPI), which indicates which control word (key) should be used to descramble the content. Each key management system has a mechanism to associate an ECM-carried key with the SPI. The key used for descrambling a packet is in the ECM with the same SPI value signaled in the IPSec packet header.

5. SIGNALING IN A/153 SYSTEMS

This section describes the mechanisms for signaling and announcing EMM and ECM streams in an A/153 system.

5.1 Conditional Access System Identification Fields

Simulcrypt key streams (EMM and ECM streams) are associated with specific conditional access systems and system operators using CA_system_id and OperatorId respectively. Signaling of ECM and EMM streams contains the CA_identification fields to signal this association (see Table 5.1).

Table 5.1 Conditional Access System and Operator Identification Fields

Syntax	No. of Bits	Format
CA_identification() {		
CA_system_id	16	uimsbf
OperatorId	16	uimsbf
}		

CA_system_Id – A 16-bit unsigned integer field that shall uniquely identify the Key Management System, and its value shall be registered at http://www.dvbservices.com/identifiers/ca_system_id.

OperatorId – A 16-bit unsigned integer field that shall uniquely identify the operator controlling this key stream. This identifier is allocated by the Key Management System. For a particular CA_system_id, it allows differentiating between two operators using the same service protection vendor.

5.2 EMM Streams

EMM streams shall be carried in EMM services.

5.2.1 EMM Streams Signaling

EMM services shall be signaled in the SMT-MH (see ATSC A/153 Part 3 [2], Section 7.3), with the SP_indicator set to '0', and the MH_service_category set to 0x04.

Furthermore, each EMM stream shall be signaled as a component having a component_level_descriptor() with component_type set to 0x43 carried in the component_level_descriptor()s loop, using the MH_component_data() shown in Table 5.2. In the case where multiple EMM streams are carried (e.g., when there are two or more conditional access systems in simultaneous use), EMM streams may be carried as multiple components of a EMM service or as multiple EMM services, or some combination thereof.

Table 5.2 Bit Stream Syntax for M/H Component Data for Service Protection Identification (Type 0x43)

Syntax	No. of Bits	Format
MH_component_data() {		
MH_service_protection_version	4	uimsbf
reserved	1	'1'
num_CA_identification	3	uimsbf
for (i=0 ; i<num_CA_identification ; ++i)		
{		
CA_identification()	32	
}		
}		

MH_service_protection_version – A 4-bit field that identifies the version of the ATSC-M/H service protection. For this version of this data structure for type 0x43, this field shall be set to 0x01.

num_CA_identification() – The number of CA_identification fields following.

CA_identification() – As defined in Section 5.1. The set of CA identification fields describes the set of conditional access systems and operators that have EMM messages carried in the stream.

5.2.2 EMM Streams Announcement Signaling

When EMM streams are present in A/153 systems, such streams shall be signaled, using a ServiceType of 128[1] in the Service fragment as in ATSC A/153, Part 4 [3], with the following additional specification: A ServiceClass of "urn: urn:oma:bcast:ext_bsc_atsc:emm:1.0:emm" [2] shall be signaled in the Access fragment. The SDP files of such services shall be compliant with ETSI 102 472 [5], in particular Section 10.2.

Services are signaled as specified in [4] and shall have kmsType set to 128[3] in the Access fragment.

5.2.2.1 ServiceType

Services signaled using ServiceType of 128 are not expected to be displayed to the user. See [4], Section 5.1.2.1.

5.3 ECM Streams

Each ECM stream shall be signaled as a component of each service for which the stream is delivering entitlement control information.

5.3.1 ECM Stream Signaling

ECM streams shall be signaled in the SMT-MH (see ATSC A/153 Part 3 [2], Section 7.3) by the addition of the MH_component_data() as shown in Table 5.3.

---

[1] This establishes the first of the OMA ServiceType "proprietary use" values, which are informatively managed for ATSC in the Code Point Registry.

[2] See http://www.openmobilealliance.org/Tech/OMNA/omna-bcast-SvcClass-registry.aspx, see also the Code Point Registry: http://www.atsc.org/cms/standards/Code-Points-Registry-Rev-22.xls .

[3] This establishes the first of the OMA kmsType "proprietary use" values, which are informatively managed for ATSC in the Code Point Registry.

Furthermore, one component_level_descriptor() with component_type 0x44 shall be carried in the component_level_descriptor() loop, using the MH_component_data() shown in Table 5.3. In the case where multiple ECM streams are associated with a service (e.g., when there are two or more conditional access systems in simultaneous use), ECM streams are associated with a conditional access system via the CA_identification field.

Table 5.3 Bit Stream Syntax for M/H Component Data for ECM Identification (Type 0x44)

Syntax	No. of Bits	Format
MH_component_data() {		
MH_service_protection_version	4	uimsbf
reserved	1	'1'
num_CA_identification	3	uimsbf
for (i=0 ; i<num_CA_identification ; ++i) {		
CA_identification()	32	
}		
ECM_stream_id	16	uimsbf
}		

MH_service_protection_version – A 4-bit field that identifies the version of the ATSC-M/H service protection. For this version of this data structure for type 0x44, this field shall be set to 0x01.

num_CA_identification() – The number of CA_identification fields following.

CA_identification() – As defined in Section 5.1. The set of CA identification fields describes the set of specific conditional access systems and operators that have ECM messages carried in the stream.

ECM_stream_id – A 16-bit unsigned integer field that shall uniquely identify this particular key stream within an M/H Service scope. This identifier is referenced by the component descriptors of protected components to indicate where keys can be found to decrypt the components. Note: This field is analogous to STKM_stream_id (see A/153, Part 3 [2], Section 7.8.1 in representing an encrypted TEK stream; see also OMA Service and Content Protection [7], Section 10.1.3).

5.3.2 ECM Streams Announcement Signaling

When ECM streams are present in A/153 systems, such streams shall be signaled in the Service fragment as in ATSC A/153, Part 4 [3]. The SDP files of such services shall be compliant with ETSI 102 472 [5], in particular Section 10.1.