Doc. TSG-717r1
22 November 2006

Proposed ATSC Standard: System Renewability Message Transport

Advanced Television Systems Committee
1750 K Street, N.W.
Suite 1200
Washington, D.C. 20006
http://www.atsc.org

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.

Table of Contents

Index of Tables and Figures

Proposed ATSC Standard: System Renewability Message Transport

1. SCOPE

This document defines the method for transport of System Renewability Messages. A System Renewability Message (SRM) is a message issued by the administrator of a Content Protection System (CPS) that, when sent to devices that use that CPS, can revoke permission of certain devices or groups of devices to obtain content protected by that CPS. Different CPSs will each have their own SRMs to maintain the integrity of their systems; e.g., in the event that device keys are stolen and cloned. Annex A provides an insertion model for SRM distribution, and Annex B presents an informative overview of how System Renewability Messages are used.

2. REFERENCES

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

2.1 Normative References

The following documents contain provisions which, through reference in this text, constitute provisions of this standard.

[1] ISO/IEC IS 13818-1:2000 (E), International Standard, Information Technology — Generic coding of moving pictures and associated audio information: systems.

[2] ETSI TR 101 162 V1.2.1 (2001-01-30), “Digital Video Broadcasting (DVB); Allocation of Service Information (SI) and Data Broadcasting Codes codes for Digital Video Broadcasting (DVB) systems,” Section 4.3; Draft; European Telecommunications Standards Institute.

3. DEFINITIONS

3.1 Acronyms and Abbreviations

The following acronyms and abbreviations are used within this document:

ATSC Advanced Television Systems Committee
bslbf bit serial, leftmost bit first
CAT Conditional Access Table
CRC cyclic redundancy check
EMM entitlement management message
PID packet identifier
rpchof remainder polynomial coefficients, highest order first
SRM System Renewability Message
TS Transport Stream
uimsbf unsigned integer, most significant bit first

3.2 Reserved Fields

reserved — Fields in this standard marked "reserved" are not to be assigned by the user, but are available for future use. Receiving devices are expected to disregard reserved fields for which no definition exists that is known to that unit. Each bit in the fields marked "reserved" is to be set to one until such time as it is defined and supported.

4. SYSTEM RENEWABILITY MESSAGE TABLE

System Renewability Messages are transported in table sections conforming to the "long" form of the MPEG-2 private_section defined in Sections 2.4.4.10 and 2.4.4.11 of ISO/IEC 13818-1 [1]. SRM data for a given provider identified by CP_provider_id may be put in multiple sections. Segmentation and utilization of the payload is at the discretion of the provider

The following constraints shall apply to the Transport Stream packets carrying the system_renewability_message_table_section ():

- PID shall be set to the value identified in the SRM_PID field of the SRM Reference Descriptor, as given in Section 5
- transport_scrambling_control bits shall be set to the value '00'

Note: the adaptation_field_control bits are unconstrained.

The bit stream syntax for the System Renewability Message Table shall be as shown in Table 4.1.

Table 4.1 Bit Stream Syntax for the System Renewability Message Table

Syntax	No. of Bits	Format
system_renewability_message_table_section() {		
table_id	8	0xE0
section_syntax_indicator	1	'1'
private_indicator	1	'1'
reserved	2	'11'
section_length	12	uimsbf
CP_provider_id	16	uimsbf
reserved	2	'11'
version_number	5	uimsbf
current_next_indicator	1	'1'
section_number	8	uimsbf
last_section_number	8	uimsbf
for(j=0; j<N; j++) {		
SRM_data()		
}		
CRC_32	32	rpchof
}		

table_id — This 8-bit field shall be set to 0xE0, identifying this section as a system_renewability_message_table_section().

section_syntax_indicator – This 1-bit field shall be set to '1' indicating the long form of the MPEG-2 private_section table.

private_indicator – This 1-bit field shall be set to '1'.

section_length – This 12-bit field shall specify the number of bytes in the system_renewability_message_table_section() immediately following this field up to and including the CRC_32 field. The value in this field shall not exceed 4093 (0xFFD).

CP_provider_id — A 16-bit field that shall identify the copy protection technology provider of SRM_data() in this table section. The value of CP_provider_id shall be unique within the same number assignment space as CA System ID values, which are assigned in ETSI TR 101 162 [2] Section 4.3 (Table 5). Copy protection system vendors are advised to contact DVB (http://www.dvb.org) for assignment of new values.

version_number – This 5-bit field shall indicate the version number of the instance of the system_renewability_message_table_section() with the given value of CP_provider_id. The version_number shall be incremented by 1 (modulo 32) when a change in the information carried within the instance of the table section occurs.

current_next_indicator – This 1-bit field shall be set to '1'.

section_number — This 8-bit field shall indicate the number of this section. The section_number of the first section in an SRM table shall be set to 0x00. The section_number shall incremented by 1 with each additional section in the SRM table. The scope of the section_number is defined by the table_id and CP_provider_id. The section_number provides for 256 x 4084 (maximum size payload in a long form section) = 1,045,504 bytes per CP_provider_id value.

last_section_number — This 8-bit field shall specify the number of the last section. The scope of the last_section_number is defined by the table_id and CP_provider_id.

SRM_data() — This data structure shall be defined by the copy protection technology provider identified in CP_provider_id.

CRC_32 – This 32-bit field shall contain the CRC value that gives a zero output of the registers in the decoder defined in ISO/IEC 13818-1[1], Annex A after processing the entire private section.

5. SRM PID SIGNALING

All SRM table sections transported within a given Transport Stream shall be carried within TS packets identified with a PID value of SRM_PID. The value of SRM_PID shall be signaled within an MPEG-2 CA Descriptor as defined in Section 2.6.16 and 2.6.17 of ISO/IEC 13818-1 [1], contained within the MPEG-2 Conditional Access Table (CAT), defined in Section 2.4.4.6 of ISO/IEC 13818-1 [1]. To distinguish this CA Descriptor used to identify SRM_PID from other CA Descriptors that may be present in the CAT, a value of 0x4ADD for CA_sytem_ID is used. An instance of an MPEG-2 CA Descriptor with this special CA_sytem_ID value shall be known as an SRM Reference Descriptor. At most one instance of the SRM Reference Descriptor shall be present in the Conditional Access Table. The bit stream syntax of the SRM Reference Descriptor shall be as shown in Figure 5.1.

Table 5.1 Bit Stream Syntax for the SRM Reference Descriptor

Syntax	No. of Bits	Format
SRM_reference_descriptor() {		
descriptor_tag	8	0x09
descriptor_length	8	uimsbf
CA_system_ID	16	0x4ADD
reserved	3	'111'
SRM_PID	13	uimsbf
for(j=0; j<N; j++) {		
additional_data()		
}		
}		

descriptor_tag — This 8-bit field shall be set to 0x09, identifying the descriptor as conforming to the syntax and semantics of an MPEG-2 Conditional Access Descriptor per Section 2.6.16 and 2.6.17 of ISO/IEC 13818-1 [1].

descriptor_length — An 8-bit count that shall indicate of the number of bytes following the descriptor_length itself.

CA_system_ID — This 16-bit field shall be set to value 0x4ADD, identifying this instance of the MPEG-2 CA Descriptor as being an SRM Reference Descriptor.

SRM_PID — This 13-bit field shall indicate the PID of Transport Stream packets carrying System Renewability Messages in this Transport Stream.

additional_data() — Optional additional information that may be defined in the future.

6. SRM T-STD MODEL

This section defines the Transport System Target Decoder (T-STD) model for SRM transport.

The buffer model block diagram is shown in Figure 6.1 below. Refer to ISO/IEC 13818-1 [1] Section 2.4.2 for context. The transport packet bytes containing SRM table sections shall not be transferred to TB_{sys}, but to TB_{SRM} as more fully described below. All other behavior of the transport buffer (TB_{SRM}) shall be as defined in 0 for other transport buffers.

t(i) is as defined in [1]. TB_{SRM} is the transport buffer for TS packets containing SRM Table sections. The transport buffer size TBS_{SRM} is 512 bytes. RX_{SRM} is the rate bytes are moved from the transport buffer to the smoothing buffer, SB_{SRM}. RX_{SRM} shall be 1×10^6 bps for SRM data. SBS_{SRM} is the size of the smoothing buffer. R_{SRM} is the rate bytes are moved out of the smoothing buffer. RX_{SRM} is 50,000 bps for SRM data.

In summary:

- t(i) is the i^{th} byte of the transport stream input (when PID matches SRM_PID) to TB_{SRM}
- TB_{SRM} is the transport buffer for the SRM stream
- TBS_{SRM} is the size of TB_{SRM} and shall be set to 512 bytes
- RX_{SRM} is the leak rate from the SRM transport buffer into the SRM smoothing buffer and shall be 1×10^6 bps
- SB_{SRM} is the smoothing buffer for the SRM stream

- SBS_{SRM} is the size of SB_{SRM} and shall be set to 1024 bytes
- R_{SRM} is the leak rate out of the smoothing buffer and shall be set to 50,000 bps

The smoothing buffer, SB_{SRM}, shall not overflow, but may underflow.

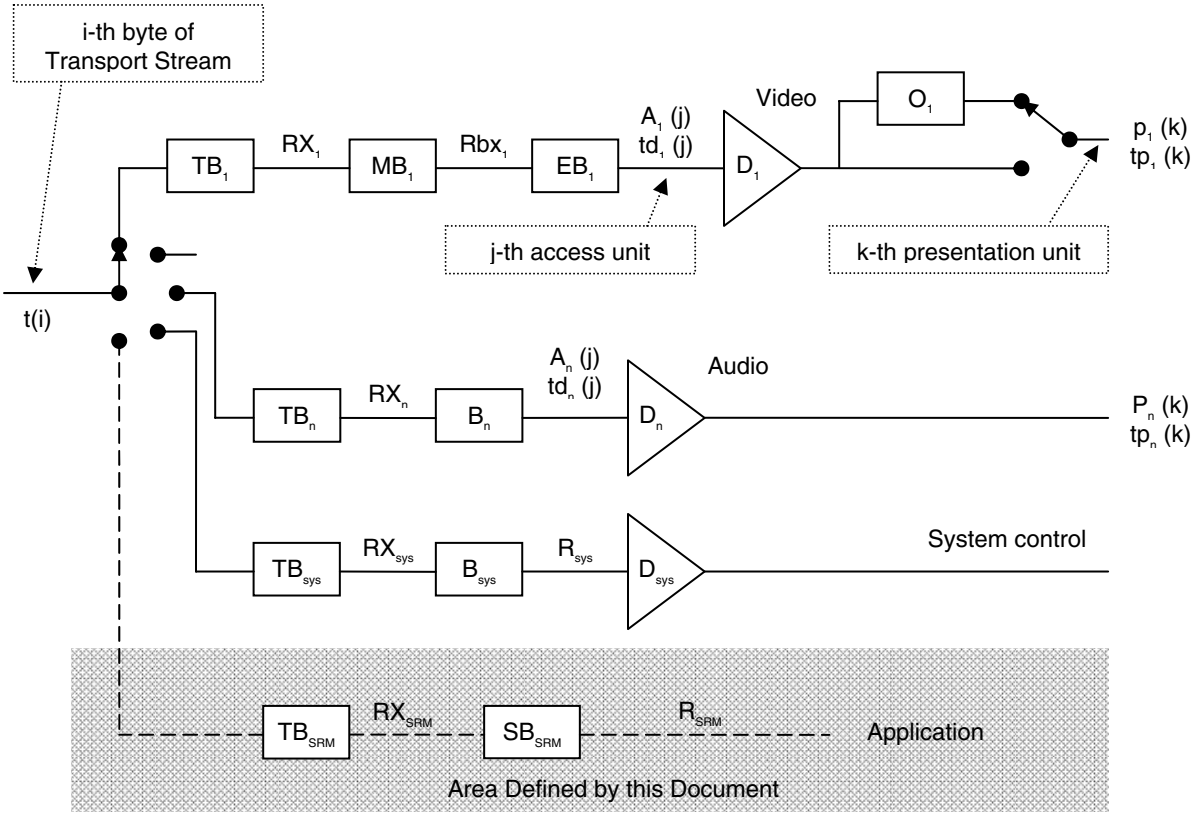

Figure 6.1 T-STD buffer model (adapted from 13818-1:2000 [1], Figure 2-1).

Annex A:
SRM Insertion Model (Informative)

Figure A1 illustrates an insertion model for System Renewability Messages flowing into a broadcast distribution chain. SRM data from Provider A and Provider B are made available on a private network or via the public Internet to a functional block called "SRM Payload Preparation/Aggregation." SRM data from Provider C is also made available to this block via a local connection. Data from the several providers is then combined and formatted into a data stream that is fed to the SRM Encapsulator, which produces an output in a format acceptable as an input to the Multiplexer.

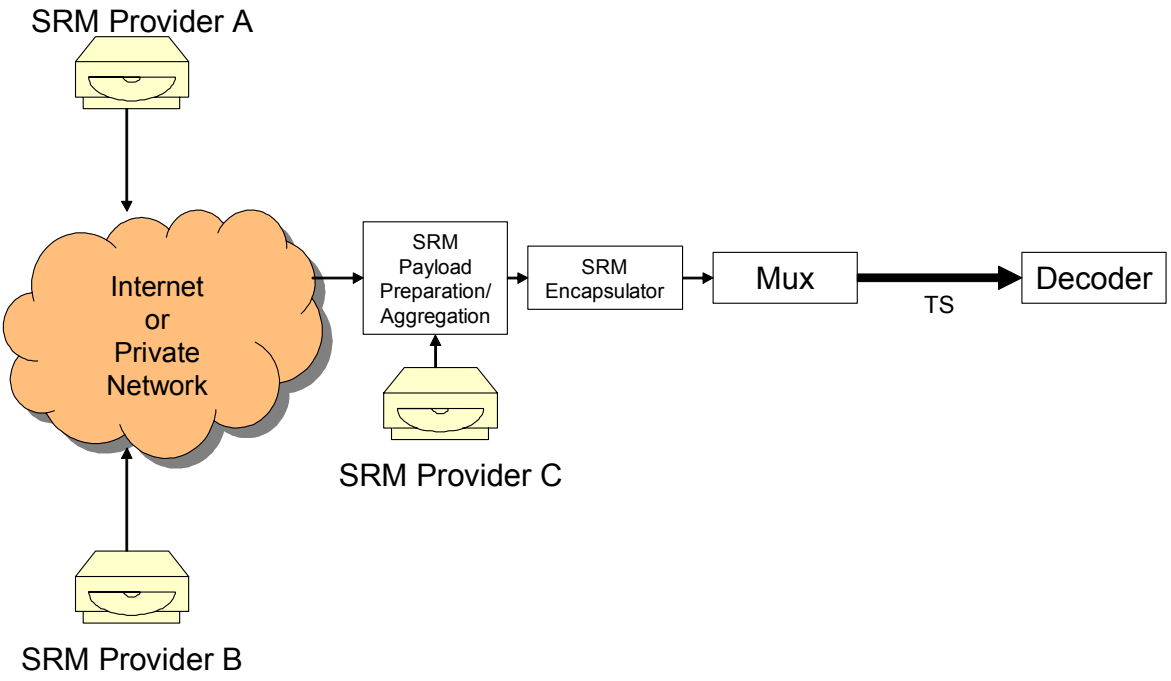

Figure A1 SRM insertion model.

Annex B:
Background (Informative)

B.1 GENERAL OVERVIEW

The continuing effectiveness of a content protection technology greatly relies on support for revocation. It must be accepted that, given enough resources and time, hackers can gain access to a content protection technology's secret device key contained within a single compliant device. This single device key can be used to produce an unlimited number of non-compliant "clone" devices that ignore all copy protection requirements. When the licensor of the content protection technology becomes aware of devices in the marketplace that contain cloned keys or certificates, they can issue a System Renewability Message that revokes this device, along with any other individual devices that contained cloned keys or certificates.

Although the term "system renewability" also can refer to the capability of a far more comprehensive renewal of the security components of a content protection system, content protection technology developers refer to their revocation list as a "System Renewability Message" (SRM). The developers of content protection technologies provide clear specifications for their System Renewability Message files. To effectuate revocation, the content protection licensor generates a new SRM file and then provides it to content providers, MVPDs, and/or broadcasters, who in turn deliver these SRMs with the content. For example, in the case of the DVD Content Scrambling System, which has approved HDCP-protected outputs, the HDCP SRM is delivered on the DVD disc as a HDCP.srm file. This SRM file is read from the DVD during playback and then conveyed to the HDCP function for SRM revocation processing. If a cloned HDCP device is connected to a DVD player playing a CSS-encrypted DVD, the cloned device can be detected during HDCP revocation processing and the DVD CSS player can stop the flow of digital content to the HDCP digital output. The DVD player continues to operate properly with its other video outputs enabled. It should be understood that content protection device key revocation does not totally disable an entire device. It only disables the particular digital protected output or the secure recording method of the device having the cloned or illegally acquired content protection device key.

Effective revocation processing relies on the latest, up-to-date SRMs being delivered in the most recent program broadcasts in order to address new "clone" attacks that surface and to correct the effect of any earlier mistaken or cured device revocations. In addition, SRMs must also be conveyed to downstream devices because some content protection technologies, such as the High-bandwidth Digital Content Protection (HDCP), do not store their revocation lists. These content protection technologies must rely on real-time processing of SRMs contained in the content to achieve effective device revocation.

An effective revocation infrastructure is a critical component in achieving the goal of facilitating the digital transition and preserving the free-to-air broadcasting system from migration of high value programming to more secure delivery systems.

B.2 ATSC BROADCAST FLAG COPY PROTECTION REVOCATION EXAMPLE

The 5C Digital Transmission Content Protection (DTCP) technology authorizes the use of 4C Content Protection for Recordable Media (CPRM) technology and the Vidi content protection

system for secure recording. The 5C DTCP, 4C CPRM and Vidi technologies authorize the use of High-bandwidth Digital Content Protection (HDCP) technology for protected digital outputs. Therefore, DTCP must preserve and convey downstream any received HDCP SRMs in the DTCP protected MPEG-2 transport stream outputs and in any subsequent CPRM-protected recordings. This is graphically described in the Figure B1, which shows an ATSC Broadcast Flag[1] compliant DTV Receiver connected using an IEEE 1394 interface to a DVD Recorder capable of making 4C CPRM-protected DVD recordings that can played out over a HDCP-protected DVI output. The HDCP SRM is preserved in the DTCP-protected MPEG-2 transport stream output from the DTV Receiver to the DVD recorder and is subsequently preserved in the CPRM-protected DVD recording. When the CPRM recording is played, the HDCP SRM is sent to the HDCP function to enable revocation processing.

Figure B1 goes on to describe how SRM preservation and conveyance is handled during serial digital copying of Marked Content. As illustrated in this example, when a DVD+RW recorder with Vidi content protection technology attempts to make a digital copy from the playback of the CPRM-protected recording using a DTCP-protected digital connection, the HDCP SRM must be conveyed and then preserved in the MPEG-2 transport stream sent to and in the MPEG-2 recording made by the Vidi recorder. In this way, when the Vidi-protected DVD recording is played, the HDCP SRM can be conveyed to the HDCP function to enable revocation processing.

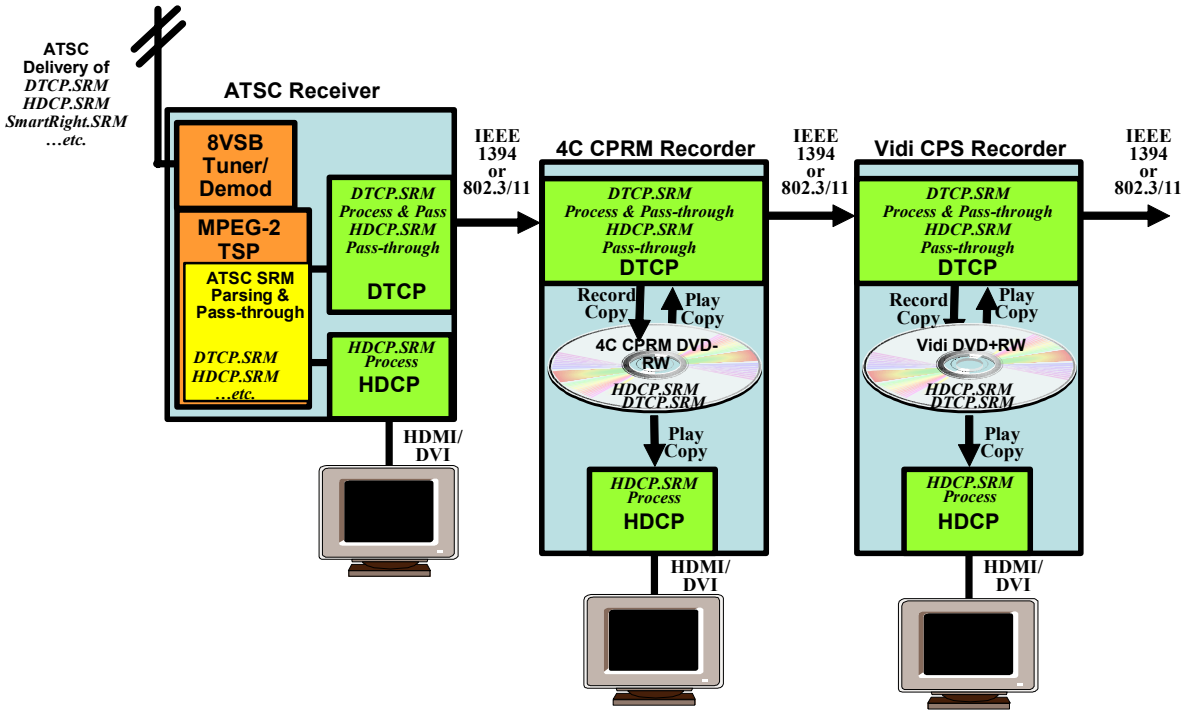

Figure B1 Broadcast Flag copy protection revocation example.

[1] The ATSC Broadcast Flag is conveyed in the rc_descriptor() defined in ATSC A/65C.

End of Document