ETSI TS 100 289 V1.1.1 (2011-09)

Digital Video Broadcasting (DVB);
Support for use of the DVB Scrambling Algorithm version 3
within digital broadcasting systems

Reference
RTS/JTC-DVB-291

Keywords
broadcasting, CA, digital, DVB, security, TV,
video

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

The present document is based on the DVB document TM3927, and it may be converted into a standard after market feedback. For this purpose, the wording of a standard (normative elements) rather than of a technical report (informative elements) has been used.

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulatory bodies, content owners and others committed to designing global standards for the delivery of digital television and data services. DVB fosters market driven solutions that meet the needs and economic circumstances of broadcast industry stakeholders and consumers. DVB standards cover all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. The consortium came together in 1993 to provide global standardisation, interoperability and future proof specifications.

Introduction

The present document describes the minimum set of common CA elements necessary to achieve interoperability between different CA Systems, in particular to support the implementation of the DVB Common Scrambling version 3 algorithm (CSA v3) within digital broadcasting systems.

1 Scope

The present document provides for support for the implementation of the DVB Common Scrambling version 3 algorithm (CSA v3) within digital broadcasting systems. Considering that there will be several Conditional Access solutions based on ISO/IEC 13818-1 (MPEG-2) [1] and the DVB specifications, the present document specifies the common signalling aspects as well as operational guidelines relevant for CA solutions. The present document provides hence the basis for co-existence of multiple Conditional Access Systems in a single Transport Stream.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 13818-1: "Information Technology - Generic coding of moving pictures and associated audio information: Systems".

[2] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

[3] ETSI TS 101 162: "Digital Video Broadcasting (DVB); Allocation of identifiers and codes for Digital Video Broadcasting (DVB) systems".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] NIST FIPS 197: "Advanced Encryption Standard".

[i.2] ATIS-0800006: "IIF Default Scrambling Algorithm".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Conditional Access (CA) system: system to control subscriber access to services, programmes and events

Service Information (SI): digital data describing the delivery system, content and scheduling/timing of broadcast data streams, etc.

NOTE: It includes MPEG-2 Program Specific Information (PSI) together with independently defined extensions.

table: comprised of a number of sections with the same value of table_id

Transport Stream (TS): data structure defined in ISO/IEC 13818-1 [1]

3.2 Abbreviations

For the purpose of the present document, the following abbreviations apply:

bslbf	bit string, left bit first
CA	Conditional Access
CAS	Conditional Access System
CSA	Common Scrambling Algorithm
DVB	Digital Video Broadcasting
ECM	Entitlement Control Message
EMM	Entitlement Management Messages
ID	IDentifier
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MPEG	Moving Picture Experts Group
NDA	Non-Disclosure Agreement
PES	Packetized Elementary Stream
PID	Packet IDentifier
PMT	Program Map Table
PSI	Program Specific Information
SMS	Subscriber Management System
TS	Transport Stream
uimsbf	unsigned integer, most significant bit first
XRC	eXtended emulation Resistant Cipher

4 The DVB Scrambling Algorithm version 3

The Scrambling Algorithm specified for common DVB applications has been designed to minimise the likelihood of piracy attack over a long period of time and thus contains highly security sensitive information. The technical details of the scrambling algorithm can only be made available to bona-fide users upon signature of a Non-Disclosure Agreement (NDA) administered by a Custodian. This clause contains an informative summary of the scrambling method and some of the implementation issues.

4.1 Technical Overview

4.1.1 Key Features

DVB-CSA v3 uses a 128-bit key (Control Word) to encrypt data blocks of any size over 16 bytes (with a granularity of 1 byte) and a descrambler requires in the order of 100 K gates in hardware (the exact number depends on the technology).

4.1.2 Encryption Algorithm

The algorithm is based on two block ciphers: a variation of the "Advanced Encryption Standard" (AES128), specified in NIST FIPS 197 [i.1], called AES' and the "eXtended emulation Resistant Cipher" (XRC), which is a DVB-confidential cipher.

4.1.3 Key Derivation Mechanism

DVB-CSA v3 uses a subset of IDEA-NXT, a block cipher published in 2004 in the academic world, which has been security assessed by several independent crypto experts. This in conjunction with the use of a DVB-confidential S-box (exclusively dedicated to DVB-CSA v3 usage) is used to derive internal keys from the control word.

4.1.4 Implementation Highlights

DVB-CSA v3 is carefully designed to be very efficiently implemented in hardware, a descrambler requiring in the order of 100 K gates.

4.2 The DVB Scrambling Algorithms Custodian

The Scrambling Algorithms for DVB applications is made available by a custodian upon signature of a Non-Disclosure Agreement and provided potential users are bone fide. The custodian is ETSI and information can be obtained by contacting:

ETSI
Algorithms & Codes
650 Route des Lucioles
06921 Sophia Antipolis
tel:+ 33 4 92 94 4216
fax: +33 4 92 38 49 04
email: algorithm&codes@etsi.org

5 Use of the scrambling algorithm in an MPEG-2 environment

This clause contains syntactical definitions and some operational requirements for MPEG-2 bitstreams allowing efficient use of the common scrambling algorithm.

5.1 Scrambling control field

The MPEG-2 Systems specification contains a scrambling control field of two bits, both in the TS packet header and in the PES packet header. The meaning of these two bits is only partially defined in MPEG-2 , as only one value is defined. Table 1 gives a full definition of the scrambling control bits in the TS packet header.

Table 1: Transport_scrambling_control values

Bit values	Description
00	No scrambling of TS packet payload (MPEG-2 compliant)
01	Reserved for future DVB use
10	TS packet scrambled with Even Key
11	TS packet scrambled with Odd Key

The first scrambling control bit now indicates whether or not the payload is scrambled. The second bit indicates the use of Even or Odd Key. If the TS packet payload is not scrambled at the TS level, scrambling of data still might be defined at the PES level. Table 2 defines the scrambling control bits in the PES packet header which are similar to those at the TS level. Similarity in the scrambling control bits and in the scrambling methods for both levels, allow efficient descrambler implementations to be realised.

Table 2: PES_scrambling_control values

Bit values	Description
00	No scrambling of PES packet payload (MPEG-2 compliant)
01	Reserved for future DVB use
10	PES packet scrambled with Even Key
11	PES packet scrambled with Odd Key

5.2 Registration of CA System ID

Some registration needs to take place on the CA_System_ID field in the MPEG-2 CA_descriptor() to indicate the various CA Systems Specifiers. The CA_System_ID field allows easy filtering of relevant CA information for a particular Digital TV receiver. TS 101 162 [3] specifies a range of 65 536 values (16-bit) for each of the CA System Specifiers. The DVB Project Office co-ordinates the allocation of new CA System Specifiers to acquire an unique range of CA_System_ID values for their private use. Typical usage of the private 16 bits assigned to each CA System Specifier is for purposes such as version indication and/or for differentiation between different SMS providers using the same CA System. The registration procedures shall adopt the information given in TS 101 162 [3]; registration is done through www.dvbservices.com.

5.3 PES level scrambling issues

Maximum flexibility in the operation of a broadcast infrastructure requires scrambling to be allowed at the PES level. In order to avoid complex implementations at the consumer receiving equipment, only a single de-scrambling circuit shall be required. Some additional constraints are defined in this clause in order to achieve PES level scrambling with a limited implementation overhead. These constraints clearly do **not** apply to unscrambled PES packets or in the case of TS-level scrambling.

Requirement 1: Scrambling shall only occur at one level (TS or PES) and is not allowed to occur at both levels simultaneously.

Requirement 2: The header of a scrambled PES packet shall not exceed 184 bytes.

Requirement 3: The TS packets carrying parts of a scrambled PES packet, shall not have Adaptation fields with the exception of TS packets containing the end of a PES packet. The TS packet carrying the end of a scrambled PES packet, may carry an Adaptation Field to align of the end of the PES packet with the end of the TS packet.

6 Trans-control issues when crossing distribution media boundaries

The Program Specific Information (PSI) part of the MPEG-2 specification contains syntactical elements defining where to find CA system information. The CA table and the Program Map Table (PMT) contain CA descriptors which has a CA_PID field to reference PID values of TS packets that are used to carry CA information such as EMMs and ECMs. It may be desirable to replace (part of) the CA information in these TS packets with other CA data at broadcast distribution media boundary. The following constraints make it possible to have a flexible replacement of the TS packets which carry CA information.

Requirement 4: All TS packets with PID values which are equal to a CA_PID value given in a CA_descriptor of the MPEG-2 specification, shall only contain CA System information. No CA information shall be carried in any other place (e.g. Adaptation Fields).

In addition, as it should be common practise anyway, two different CA suppliers should not have common CA_PID values in the same TS.

These constraints are sufficient to allow efficient trans-control to occur at broadcast delivery media boundary by filtering out CA data and replacing it with new CA information.

7 Conditional Access (CA) data

This clause specifies a section mechanism as defined in the ISO/IEC 13818-1 [1] for the transport of Conditional Access (CA) information, such as ECMs, EMMs and future entitlement data. The structure of this CA information is specific to each CA System Specifier. Two types of tables are identified by two different table_id values (see table 4), which are intended for the transmission of ECMs. The header of the CA_message_section() may be used for filtering. The ISO/IEC 13818-1 [1] describes how sections are carried in TS packets. CA_message_sections shall be treated as ISO/IEC 13818-1 [1] private_sections, when inserting them into a TS.

The CA message sections specified in table 3 shall have a maximum length of 256 bytes.

Table 3: Syntax for the CA Message Table (CMT)

Syntax	No. of bits	Identifier
CA_message_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
DVB_reserved	1	bslbf
ISO_reserved	2	bslbf
CA_section_length	12	uimsbf
for(i=0; I<N; i++) {		
CA_data_byte	8	bslbf
}		
}		

Semantics for the CMT:

table_id: See table 4.

Table 4: Allocation of table identifiers

table_id value	Description
0x003 to 0x3F	MPEG_reserved
0x40 to 0x7F	DVB_reserved
0x80	CA_message_section, ECM
0x81	CA_message_section, ECM
0x82 to 0x8F	CA_message_section, CA System private
0x90 to 0xFE	user defined
0xFF	MPEG_reserved

section_syntax_indicator: This 1-bit indicator shall always be set to "0".

DVB_reserved: This term indicates that the field is already or may be used in the future for DVB applications and therefore shall not be used for private applications.

MPEG_reserved: This term indicates that the value is already or may be used in the future for ISO defined extensions and therefore is not be specified by DVB.

CA_section_length: This 12-bit field specifies the number of bytes that follow the section_length field up to the end of the section.

CA_data_byte: This 8-bit field carries private CA information. Up to the first 17 CA_data_bytes may be used for address filtering.

A range of 16 table_id values is available for CA_message_sections carrying different types of Conditional Access information. Two values of the table_id field (0x80 and 0x81) are reserved for transmission of ECM data. A change of these two table_id values signals that a change of ECM contents has occurred. This change condition can be used for filtering of Conditional Access information.

8 Scrambling descriptor

This clause specifies a section mechanism as defined in EN 300 468 [2] for the transport of signalling information to indicate which CSA is in use, and if CSA3, then which mode is indicated.

The scrambling descriptor indicates the selected mode of operation for the scrambling system. It is located in the program map section at the program loop level.

Table 5: Scrambling_descriptor

Syntax	Number of bits	Identifier
scrambling_descriptor(){		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
scrambling_mode	8	uimsbf
}		

Semantics for the scrambling_descriptor:

scrambling_mode: This 8-bit field identifies the selected mode of the scrambling algorithm (see table 6). The technical details of the scrambling algorithm are available only to bona-fide users upon signature of a Non Disclosure Agreement (NDA) administered by the DVB Common Scrambling Algorithm Custodian.

Table 6: scrambling_mode coding

scrambling_mode	Description
0x00	Reserved for future use.
0x01	This value indicates use of DVB-CSA v1. It is the default mode and is to be used when the scrambling descriptor is not present in the program map section.
0x02	This value indicates use of DVB-CSA v2.
0x03	This value indicates use of DVB-CSA v3 in standard mode.
0x04	This value indicates use of DVB-CSA v3 in minimally enhanced mode.
0x05	This value indicates use of DVB-CSA v3 in fully enhanced mode.
0x06 to 0x6F	Reserved for future use.
0x70 to 0x7F	ATIS defined (ATIS-0800006 [i.2], see annex J).
0x80 to 0xFE	User defined.
0xFF	Reserved for future use.

Mixing of different scrambling modes within the same Transport Stream:

- This situation may occur when a TS is made by multiplexing two or more independent TS streams.

Mixing of different scrambling modes within the same service at the same time:

- This is not allowed. The same mode shall be used by all scrambled components of a service at the same time.

Change of scrambling mode over time for a given service (e.g. from event to event):

- This situation may occur at any time, for instance when broadcasting events that were stored in scrambled mode or when inserting a local programme. Transitions should not be expected to be seamless.

Annex A (informative): Bibliography

- ISO/IEC 13818-2: "Information technology - Generic coding of moving pictures and associated audio information: Video".
- ISO/IEC 13818-3: "Information technology - Generic coding of moving pictures and associated audio information - Part 3: Audio".
- ISO/IEC 13818-4: "Information Technology - Generic coding of moving pictures and associated audio information: Compliance".
- ETSI TS 101 211: "Digital Video Broadcasting (DVB); Guidelines on implementation and usage of Service Information (SI)".
- ETSI TS 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".

History

Document history		
Edition 1	October 1996	Publication as ETR 289
V1.1.1	September 2011	Publication