Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems

DVB Document A125

July 2008

Contents

Introduction

This BlueBook addresses the introduction of a more robust Common Scrambling Algorithm (CSA) for incorporation into new receiving devices as soon as possible, such that in a 7-10 year timeframe, most if not all receiving devices could be expected to be capable or operating with the new, updated algorithm (as well as being backwards compatible with the existing CSA).

The Conditional Access System (CAS) is a very sensitive area, and this TR describes the minimum set of common CA elements necessary to achieve interoperability between different CA Systems. It is reasonable to expect these common CA elements to be incorporated in every piece of consumer receiver equipment for digital TV.

1 Scope

The present document specifies the new common DVB Conditional Access elements. It was developed to address the fact that the original CSA was created with an expected lifetime of ten years before any likelihood of compromise through brute force attack was forseen.

It was developed principally to provide support for a wide range of Conditional Access Systems (CASs) which are based on ISO/IEC 13818-1 (MPEG-2) [1] and the DVB specifications. The present document specifies those aspects which are required for co-existence of multiple Conditional Access Systems in a single data stream.

2 References

For the purposes of the present document, the following references apply:

[1] ISO/IEC 13818-1: "Information Technology - Generic coding of moving pictures and associated audio: Systems, Recommendation H.222.0".

[2] ISO/IEC 13818-4: "Information Technology - Generic coding of moving pictures and associated audio: Compliance".

[3] TR 101 162: "Digital broadcasting systems for television, sound and data services; Allocation of Service Information (SI) codes for Digital Video Broadcasting (DVB) systems".

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

[5] TR 101 211: "Digital broadcasting systems for television; Guidelines on the implementation and usage of Service Information (SI)".

[6] TR 101 154: "Digital Video Broadcasting (DVB); Implementation guidelines for the use of MPEG-2 Systems, Video and Audio in satellite, cable and terrestrial broadcasting applications".

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
e.g. Videoguard, NagraVision

Custodian: Distribution authority for the DVB Scrambling Algorithm.

MPEG-2: Refers to the standard ISO/IEC 13818:

- Systems coding is defined in part 1
- Video coding is defined in part 2
- Audio coding is defined in part 3

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

NOTE: It is the basis of the DVB standards.

3.2 Abbreviations

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

AF	Adaptation Field
bslbf	bit string, left bit first
CA	Conditional Access
CAS	Conditional Access System
CATV	Community Access TeleVision
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

4 The DVB Scrambling Algorithm

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 a 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 100K 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, called AES' and the « eXtended emulation Resistant Cipher » (XRC), which is a DVB-confidential cipher.

4.1.3 Key Derivation Mechanism

DVB-CSA3 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.

4.1.5 Implementation Highlights

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

4.2 The DVB Scrambling Algorithm custodian

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

European Telecommunications Standards Institute (ETSI)

Administration Department

F-06921 Sophia Antipolis Cedex

FRANCE

Tel.: +33 4 92 94 42 00

Fax: +33 4 93 65 47 16

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

This clause contains syntactical definitions and some operational recommendations 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. ETR 162 [3] specifies a range of 256 values (8-bit) for each of the CA System Specifiers. ETSI, as Custodian, 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 8 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 ETR 162 [3].

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 subclause in order to achieve PES level scrambling with a limited implementation overhead. These recommendations clearly do **not** apply to unscrambled PES packets or in the case of TS-level scrambling.

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

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

Recommendation 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.

Recommendation 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).

Recommendation 5: Two different CA suppliers shall not have common CA_PID values in the same TS.

These recommendations 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
0x00 - 0x02	MPEG specified
0x03 - 0x3F	MPEG_reserved
0x40 - 0x72	V2-SI specified
0x73 - 0x7F	DVB_reserved
0x80	CA_message_section, ECM
0x81	CA_message_section, ECM
0x82 - 0x8F	CA_message_section, CA System private
0x90 - 0xFE	private
0xFF	ISO_reserved

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

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

ISO_reserved: The term "ISO_reserved" indicates that the value may be used in the future for ISO defined extensions and therefore is not be specified by DVB.

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

CA_data_byte: This is an 8-bit field which 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 the ETSI EN 300 468 [4] 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 76: 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 77). 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 77: scrambling_mode coding

scrambling_mode	Description
0x00	reserved for future use
0x01	This value indicates use of DVB-CSA1. It is the default mode and shall be used when the scrambling descriptor is not present in the program map section.
0x02	This value indicates use of DVB-CSA2.
0x03	This value indicates use of DVB-CSA3 in standard mode.
0x04	This value indicates use of DVB-CSA3 in minimally enhanced mode.
0x05	This value indicates use of DVB-CSA3 in fully enhanced mode.
0x06 to 0x6F	reserved for future use
0x70 to 0x7F	ATIS defined (ATIS-0800006, 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.