Basic Interoperable Scrambling System (BISS)

March 2000

European Broadcasting Union
Case postale 45
Ancienne Route 17A
CH-1218 Grand-Saconnex
Geneva, Switzerland
techreview@ebu.ch

EBU•UER

Summary

The rapid increase in the use of DSNG technology during recent years has spawned the development of several different proprietary security mechanisms. However, the widespread acceptance of DVB standards has made it possible to provide a security mechanism which offers interoperability between DSNG equipment from different vendors.

A standard mechanism for scrambling DSNG transmissions has already been agreed by the DVB Crypto Experts Group, based on the DVB Common Scrambling Algorithm. This document describes the additional mechanisms that are required for conditional access to DSNG transmissions, at the same time allowing full interoperability between different makes of DSNG equipment.

This document was approved by EBU project group N/DSNG-CA during their meeting in Villars, Switzerland, on 27 January 2000.

The project group wishes to thank James Cunningham, from Tandberg Television, for his heavy involvement in drafting the document.

Contents

List of Figures

List of Tables

1. Introduction

1.1. Overview

The rapid increase in the use of Digital SNG (DSNG) technology during recent years has resulted in the offering of digital codec equipment by a number of vendors. At the same time, the absence of standard methods for securing and scrambling DSNG broadcasts has spawned the development of several different proprietary security mechanisms. For instance, RAS – developed by Tandberg Television – is used in the mobile DSNG environment, as well as in various fixed contribution systems, including the EBU *Eurovision* network.

The widespread acceptance of DVB standards makes possible the proposal and provision of a security mechanism which offers interoperability between the equipment of different DSNG vendors. This would enable broadcasters to combine equipment from among several vendors, while making systems more future-proof.

The DVB Crypto Experts Group has agreed upon a standard mechanism for scrambling DSNG transmissions, based upon the DVB Common Scrambling Algorithm. This document proposes the additional mechanisms required for conditional access to allow interoperability of DSNG vendors' equipment.

1.2. Nomenclature

Throughout this document the term **Scrambler** relates to the overall mechanisms required to meet the DVB Common Scrambling Specification (Part 2).

Throughout this document the term **Scrambling Module** relates to the Super Scrambling Mechanisms required to meet the DVB Common Scrambling Specification (Part 2).

Throughout this document the term **SAM** relates to the Scrambling Authorization Module as required to meet the DVB Common Scrambling Specifications (Parts 2 and 3).

Throughout this document the term **Session Key** relates to the key that is unique and constant for the duration of the transmission. This may be a fixed CW, used for scrambling the transport stream directly or for adding a level of indirection – a key which is used to scramble changing CWs within Entitlement Control Messages.

Throughout this document the term **Session Word** relates to the word from which the Session Key is derived, i.e. the Session Word is not used directly in the scrambling process, but is transformed by some mechanism into the Session Key.

1.3. Security Requirements

The DSNG model requires the direct entry of a Session Word at the transmitter and receiver, to control access to the transmission. The sender and receiver(s) of the transmission share the Session Word, such that only the intended parties will receive the transmission, outlined as follows:

1) Session Word entered at the DSNG unit in the field.
2) Session Word entered at the receiving IRDs.
3) If the Session Words are the same, then the IRDs are able to decrypt the broadcast.

4) If the Session Words are different, the broadcast is not received.

The security requirements for fixed contribution systems are somewhat different to the DSNG model. The secure exchange of Session Keys is fundamental to such systems and is achievable. For fixed systems requiring interoperability with DSNG units, external control systems may be employed to allow the transmission of Entitlement Management Messages (EMMs) for securely exchanging Session Keys between transmitting and receiving sites. This model works for transmission sites that are part of the fixed network, but when receive sites are accepting a transmission from a DSNG unit, the operation must revert to the direct-entry method described above.

2. Functional Requirements

2.1. Modes of Operation

The Scrambler must be capable of supporting the following four modes of operation:

- ⇨ **Mode 0**: No scrambling.
- ⇨ **Mode 1**: All components are scrambled by a fixed CW.
- ⇨ **Mode 2**: All components are scrambled by a single CW sequence. The Scrambling Module fixes a CW from the sequence for the duration of the crypto-period.
- ⇨ **Mode 3**: Each component may be scrambled by a different CW sequence as in Mode 2.

The Scrambler shall implement the Super Scrambling operations as defined in the DVB Common Scrambling Specification (Part 2). The scrambling mechanism shall be applied at Transport level only.

To support the various modes of operation, the Scrambler must be capable of inserting ECM streams into the multiplex and these streams shall be appropriately identified within the PMT. The use of EMM streams has no application within the modes of operation described within this document; however, DSNG-compatible equipment may utilize such streams when employed in a fixed network architecture.

A CAT shall be present in the multiplex for modes 1, 2 and 3, although the table shall be empty, as no EMM stream will be present. Again, DSNG-compatible equipment which is employed within a fixed network system, utilizing EMM streams, shall identify them appropriately within the CAT.

A Scrambler that only supports a subset of the defined modes of operation must do so according to an imposed hierarchy. A Scrambler providing support for mode 2, must also support modes 0 and 1. Likewise, a Scrambler providing support for mode 3, must also support modes 0, 1 and 2.

2.2. Mode 0

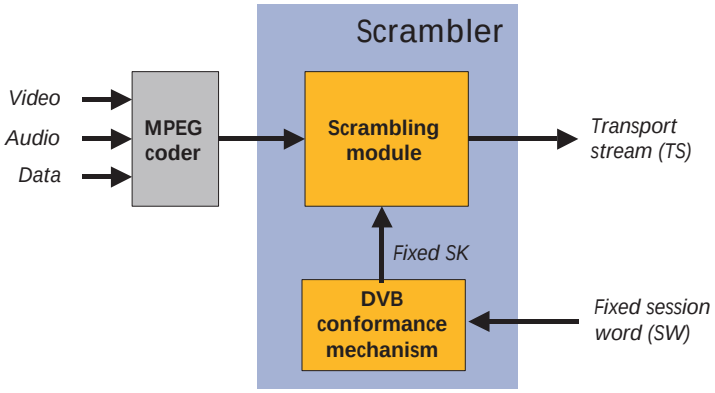
The scrambler must be capable of disabling the scrambling operation. In this mode there will be no *CA_descriptor* in the PMT and no ECM stream. The *Transport_Scrambling_Control* bits of the Transport Packets will be set to “00”.

2.3. Mode 1

2.3.1. Overview

In this mode, the Scrambler uses a fixed Control Word (CW) for the duration of the transmission. The operator shall enter a Session Word, which is transformed into the Session Key (SK) for use by the Scrambling Module. In this mode, the terms Session Word and Session Key are synonymous with the terms Control Word and Common Key from the DVB Common Scrambling specifications, respectively. An overview is given in *Fig. 1*.

Figure 1
Overview – Mode 1.



The SW is a 48-bit word which is transformed by the Scrambler into a 64-bit SK using the Conformance Mechanism defined as part of the DVB Common Scrambling specifications.

The 48-bit SW is first mapped to the 64-bit CW by the Scrambler, prior to applying the Conformance Mechanism. The mapping of bytes between the 48-bit SW and the 64-bit CW is given in *Table 1*.

Table 1
SW to fixed CW mapping.

64-bit CW	48-bit SW
CW(1)	SW(1)
CW(2)	SW(2)
CW(3)	SW(3)
CW(4)	see note [a]
CW(5)	SW(4)
CW(6)	SW(5)
CW(7)	SW(6)
CW(8)	see note [b]

a. CW(4) is derived from SW(1)..SW(6) by the DVB-defined Conformance Mechanism.

b. CW(8) is derived from SW(1)..SW(6) by the DVB-defined Conformance Mechanism.

In this mode there will be a *CA_descriptor* in the PMT, present at programme level, but no ECM stream. A single unique *CA_System_ID* is assigned to identify mode 1.

The *Transport_Scrambling_Control* bits of the Transport Packets shall be set to “10”.

Manual entry of the SW shall be in Hexadecimal, with the digits entered most-significant-nibble first, i.e. from left to right as viewed in hexadecimal notation.

> For example, 0xA13DBC42908F, would be entered in the following sequence: A,1,3,D,B,C,4,2,9,0,8,F.

Remote entry of the SW shall also be provided, although the specification of this interface is beyond the scope of this document.

The Scrambler shall ensure that the SK used by the Scrambling Module cannot be changed more than 10 times in a 5 minute period and that there is a minimum of 10 seconds between changes.

2.3.2. CA_descriptor

The *CA_descriptor* which must be present in the PMT to support mode 1 is defined in *Table 2*.

Semantics:

CA_system_ID: this is a 16-bit field indicating the type of CA system applicable for the associated ECM streams. The value of this field for mode 1 is 0x2600.

CA_PID: this is a 13-bit field indicating the PID of the Transport Stream packets that shall contain the ECM information. For mode 1, no ECM information is required, so this field shall contain the value 0x1FFF.

Table 2
Conditional Access Descriptor – Mode 1.

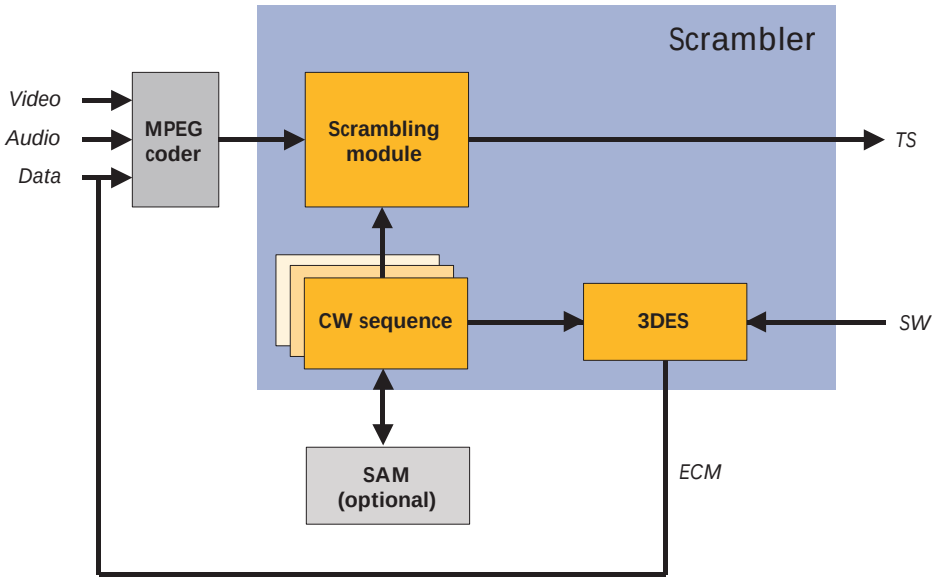
Syntax	No. of bits	Identifier
CA_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
}		

2.4. Modes 2 and 3

2.4.1. Overview

In this mode, the Scrambler uses a variable CW for a particular transmission (Mode 2), or for the components making up a transmission (Mode 3). An overview is given in *Fig. 2*.

Figure 2
Overview – Modes 2 and 3.



To support Modes 2 and 3, DVB-compliant CW sequences must be produced in advance and stored locally to the Scrambler, e.g. in a FLASH memory device. The Scrambler shall fix the next CW from the sequence of CWs in the Scrambling Module for the duration known as the *crypto-period* (typically a few seconds). The CWs shall be encrypted and transmitted within an ECM stream, protected by the Session Key. The SAM, if present, shall only perform CW authentication and not CW generation.

The CWs shall be encrypted using DES in ABC EDE 3DES mode without chaining (ECB) and a key size of 168 bits. In order to make this algorithm exportable, only 56 bits of the key shall be the operator-dependent Session Word, while the other 112 bits shall be constant.

In mode 2 there will be a *CA_descriptor* in the PMT, present at programme level, which identifies the ECM stream for the CW sequence. In mode 3 there will be a *CA_descriptor* in the PMT, present for each component, which identifies the ECM stream for the CW sequence of

that component [1]. A single unique *CA_System_ID* is assigned to identify both modes 2 and 3. The two modes are distinguished only by the position of the *CA_descriptors* in the PMT as described above.

For both modes, the *Transport_Scrambling_Control* bits of the Transport Packets may be set to "10" or "11" depending on whether the even or odd key is being used, respectively.

2.4.2. Control Word Encryption

The 168-bit Session Key used for 3DES encryption of the CW is obtained as follows:

1) A 56-bit Session Word requiring 14 hexadecimal digits provided by the operator.

2) A Key Escrow (KE) of 112 bits.

3) **1** and **2** are concatenated and the resulting 168 bits are used as the Session Key for the 3DES encryption.

SK(167..0) = [KE & SW]

i.e. The KE forms the msbs of the SK, and the SW forms the lsbs of the SK.

⇨ SK(167..56) = KE(111..0)

⇨ SK(55..0) = SW(55..0)

⇨ If KE = 0x00000000000000000000000000000 and SW = 0x11223344556677, then SK = 0x00000000000000000000000011223344556677.

The mapping between the SK and the ABC 3DES key is shown in *Table 3*. Note that SK uses engineering notation (i.e. msb = 55, lsb = 0) while 3DES uses FIPS notation (i.e. msb = 1, lsb = 56).

Table 3
SK to 3DES Key Mapping.

	A(1..56)	B(1..56)	C(1..56)
DES Mode	E	D	E
Session Key	SK(167..112)	SK(111..56)	SK(55..0)

The standard allows for up to 256 KE options, such that during a transmission a particular KE may be used to secure the session. The KE option is identified within the *fixed_bits_option* field of the ECM, so that a descrambler may select the same KE as used by the scrambler of the transmission.

For interoperability it is essential that the scrambler and descrambler share the same KE for any particular session. The specific application of the KE options is beyond the scope of this specification. However, in order to allow for true interoperability, a KE value of "00000000000000000000000000000" is assigned for *fixed_bits_option* = "0x00" (the default).

1. In mode 3, it should be possible to enter a separate Session Word for each component that requires specific entitlement control.

The bit mapping between the CW and the 3DES cypher block is shown in *Table 4*. Note that CW uses engineering notation (i.e. msb = 63, lsb = 0) while 3DES uses FIPS notation (i.e. msb = 1, lsb = 64).

Table 4
CW to 3DES Cypher Block Mapping.

3DES(1) <= CW(63)	3DES(33) <= CW(31)
3DES(2) <= CW(62)	3DES(34) <= CW(30)
3DES(3) <= CW(61)	3DES(35) <= CW(29)
3DES(4) <= CW(60)	3DES(36) <= CW(28)
3DES(5) <= CW(59)	3DES(37) <= CW(27)
3DES(6) <= CW(58)	3DES(38) <= CW(26)
3DES(7) <= CW(57)	3DES(39) <= CW(25)
3DES(8) <= CW(56)	3DES(40) <= CW(24)
3DES(9) <= CW(55)	3DES(41) <= CW(23)
3DES(10) <= CW(54)	3DES(42) <= CW(22)
3DES(11) <= CW(53)	3DES(43) <= CW(21)
3DES(12) <= CW(52)	3DES(44) <= CW(20)
3DES(13) <= CW(51)	3DES(45) <= CW(19)
3DES(14) <= CW(50)	3DES(46) <= CW(18)
3DES(15) <= CW(49)	3DES(47) <= CW(17)
3DES(16) <= CW(48)	3DES(48) <= CW(16)
3DES(17) <= CW(47)	3DES(49) <= CW(15)
3DES(18) <= CW(46)	3DES(50) <= CW(14)
3DES(19) <= CW(45)	3DES(51) <= CW(13)
3DES(20) <= CW(44)	3DES(52) <= CW(12)
3DES(21) <= CW(43)	3DES(53) <= CW(11)
3DES(22) <= CW(42)	3DES(54) <= CW(10)
3DES(23) <= CW(41)	3DES(55) <= CW(9)
3DES(24) <= CW(40)	3DES(56) <= CW(8)
3DES(25) <= CW(39)	3DES(57) <= CW(7)
3DES(26) <= CW(38)	3DES(58) <= CW(6)
3DES(27) <= CW(37)	3DES(59) <= CW(5)
3DES(28) <= CW(36)	3DES(60) <= CW(4)
3DES(29) <= CW(35)	3DES(61) <= CW(3)
3DES(30) <= CW(34)	3DES(62) <= CW(2)
3DES(31) <= CW(33)	3DES(63) <= CW(1)
3DES(32) <= CW(32)	3DES(64) <= CW(0)

2.4.3. Entitlement Control Message

The ECM is in the form of a section as defined by ISO/IEC 13818-1 [1]. The message format for an ECM, as part of this standard, is given in *Table 5*.

Table 5
Entitlement Control Message Section.

Syntax	No. of bits	Identifier
entitlement_control_message_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
DVB_reserved	1	bslbf
ISO_reserved	2	bslbf
CA_section_length	12	uimsbf
fixed_bits_option	8	uimsbf
even_cw_encrypted	64	bslbf
odd_cw_encrypted	64	bslbf
for (i=0; i<N; i++) {		
CA_data_byte	8	bslbf
}		
}		

Semantics:

table_id: this field can assume the value of 0x80 or 0x81 to identify it as an ECM section. When the value of the *table_id* changes, it indicates a change of the contents of the ECM.

fixed_bits_option: this identifies the key escrow option from the set of fixed bits (the default = "0x00").

even_cw_encrypted: this is the 3DES-encrypted Even CW.

odd_cw_encrypted: this is the 3DES-encrypted Odd CW.

Timing the playout of a new ECM is a balance between reliability and security. By playing out an ECM well in advance of the crypto-period with which it is associated, the system is more reliable. However, if the ECM appears too much in advance, then an attack on the ECM stream is much easier. To achieve a proper balance, the repetition rate of ECMs shall be 10 per second and the playout shall not be mandated but constrained, with the crypto-period limited to a minimum of 500 ms. Thus, an ECM relating to a new crypto-period must be played out in advance by at least the minimum crypto-period.

The playout of a new ECM must be such that a receiver can process it in time for the next crypto-period. If reliability is required over security, the ECM for a particular crypto-period may be played out for the entirety of the prior crypto-period.

2.4.4. CA_descriptor

The *CA_descriptor* which must be present in the PMT to support modes 2 and 3 is defined in *Table 6*.

Table 6
Conditional Access Descriptor – Modes 2 and 3.

Syntax	No. of bits	Identifier
CA_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
}		

Semantics:

CA_system_ID: this is a 16-bit field, indicating the type of CA system applicable for the associated ECM streams. The value of this field for modes 2 and 3 is 0x2601. A single *CA_system_ID* identifies both modes; the modes are distinguished by the location of the *CA_descriptor(s)* within the PMT.

CA_PID: this is a 13-bit field, indicating the PID of the Transport Stream packets that shall contain the ECM information.

3. References

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

[2] ETR 162: **Digital broadcasting systems for television, sound and data services; Allocation of Service Information (SI) codes for Digital Video Broadcasting (DVB) systems**.

[3] ETR 289: **Digital broadcasting systems for television, sound and data services; Support for use of scrambling and conditional access (CA) within digital broadcasting systems**.

[4] ETS 300 468: **Digital broadcasting systems for television, sound and data services; Specification for Service Information (SI) in Digital Video Broadcasting (DVB) systems**.

[5] FIPS PUB 46-2: **Data Encryption Standard**.

[6] FIPS PUB 46-3: **Data Encryption Standard**.

[7] FIPS PUB 81: **DES Modes of Operation**.

[8] ANSI X9.52: **Triple Data Encryption Algorithm Modes of Operation**.

[9] http://www.etsi.org/: **DVB Common Scrambling Specifications**.

4. Abbreviations

3DES	Triple DES
ABC	DES Keys A, B, C
bslbf	Bit String, Left Bit First
CA	Conditional Access
CAT	Conditional Access Table
CK	Common Key
CW	Control Word
DES	Data Encryption Standard
DSNG	Digital SNG
ECB	Electronic Codebook
ECM	Entitlement Control Message
EDE	Encode, Decode, Encode
EMM	Entitlement Management Message
KE	Key Escrow
lsb	Least Significant Bit
LSB	Least Significant Byte
msb	Most Significant Bit
MSB	Most Significant Byte
PSI	Programme Specific Information
PMT	Programme Map Table
SAM	Scrambling Authorization Module
SK	Session Key
SNG	Satellite News Gathering
SW	Session Word
uimsbf	Unsigned Integer, Most Significant Bit First