INTERNATIONAL TELECOMMUNICATION UNION

**ITU-T**

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

**J.96**

(07/2002)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Ancillary digital services for television transmission

# Technical method for ensuring privacy in long-distance international MPEG-2 television transmission conforming to ITU-T Recommendation J.89

ITU-T Recommendation J.96

ITU-T J-SERIES RECOMMENDATIONS

**CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS**

| | |
|---|---|
| General Recommendations | J.1–J.9 |
| General specifications for analogue sound-programme transmission | J.10–J.19 |
| Performance characteristics of analogue sound-programme circuits | J.20–J.29 |
| Equipment and lines used for analogue sound-programme circuits | J.30–J.39 |
| Digital encoders for analogue sound-programme signals | J.40–J.49 |
| Digital transmission of sound-programme signals | J.50–J.59 |
| Circuits for analogue television transmission | J.60–J.69 |
| Analogue television transmission over metallic lines and interconnection with radio-relay links | J.70–J.79 |
| Digital transmission of television signals | J.80–J.89 |
| **Ancillary digital services for television transmission** | **J.90–J.99** |
| Operational requirements and methods for television transmission | J.100–J.109 |
| Interactive systems for digital television distribution | J.110–J.129 |
| Transport of MPEG-2 signals on packetised networks | J.130–J.139 |
| Measurement of the quality of service | J.140–J.149 |
| Digital television distribution through local subscriber networks | J.150–J.159 |
| IPCablecom | J.160–J.179 |
| Miscellaneous | J.180–J.199 |
| Application for Interactive Digital Television | J.200–J.209 |

*For further details, please refer to the list of ITU-T Recommendations.*

# ITU-T Recommendation J.96

## Technical method for ensuring privacy in long-distance international MPEG-2 television transmission conforming to ITU-T Recommendation J.89

### Summary

This ITU-T Recommendation describes a Basic Interoperable Scrambling System (BISS-E) for use on digital contribution circuits (satellite, DSNG, etc.) compliant with ITU-T Rec. J.89, which uses fixed keys. BISS-E uses encrypted Session Words and allows centrally managed conditional access.

### Source

ITU-T Recommendation J.96 was revised by ITU-T Study Group 9 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 July 2002.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

# CONTENTS

# ITU-T Recommendation J.96

# Technical method for ensuring privacy in long-distance international MPEG-2 television transmission conforming to ITU-T Recommendation J.89

## 1 Scope

This Recommendation constitutes a common standard for a conditional access system for long distance international transmission of digital television according to MPEG Professional Profile (4:2:2).

The rapid increase in the use of Digital Satellite News Gathering (DSNG) technology has resulted in the availability of digital codec equipment from a number of vendors. At the same time, the absence of standard methods for the securing and scrambling of DSNG broadcasts has spawned the development of several different proprietary security mechanisms.

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

The Basic Interoperable Scrambling System (BISS) is based on the DVB-CSA specification [1], and the use of fixed clear keys called Session Words (SWs). BISS specification Mode 1 is used for DSNG.

BISS specification Mode E (BISS with Encrypted keys – referred to as BISS-E) introduces an additional mechanism to accept the insertion of Encrypted Session Words (ESWs) while, at the same time, conserving interoperability. This mechanism is backward-compatible with BISS specification Mode 1.

## 2 Informative reference

– EBU Technical Document: Tech 3292 rev.2 (2002), *BISS-E – Basic Interoperable Scrambling System with Encrypted keys*.

## 3 Definitions

This Recommendation defines the following terms:

**3.1 scrambler**: relates to the overall mechanisms required to meet the DVB-CSA specification.

**3.2 session word**: relates to the word assigned during a transmission by the Management Centre.

**3.3 unit**: relates to a device for which this Recommendation might apply.

**3.4 management centre**: refers to an organization controlling or managing the conditional access system.

**3.5 decryption function**: refers to a logical function used to decrypt the Encrypted Session Words, with the help of a key.

**3.6 interoperable function**: refers to a decryption function that shall be embedded in all units.

The bits in binary numbers or sequences are numbered from the left, according to engineering notation. Bit 0 is on the right and is the least significant one; the bit on the left is the most significant one.

Here is an example of engineering notation for an n-bit number:

$$b_{n-1}b_{n-2} \ldots b_1b_0$$

## 4 Abbreviations

This Recommendation uses the following abbreviations:

| | |
|---|---|
| BISS | Basic Interoperable Scrambling System |
| bslbf | Bit String, Left Bit First |
| CA | Conditional Access |
| CAT | Conditional Access Table |
| CSA | (DVB) Common Scrambling Algorithm |
| CW | Control Word |
| DES | Data Encryption Standard |
| DSNG | Digital Satellite News Gathering |
| DVB | Digital Video Broadcasting |
| ECB | Electronic Codebook |
| ECM | Entitlement Control Message |
| EMM | Entitlement Management Message |
| ESW | Encrypted Session Word |
| lsb | Least Significant Bit |
| LSB | Least Significant Byte |
| MC | Management Centre |
| msb | Most Significant Bit |
| MSB | Most Significant Byte |
| PID | Packet Identification number |
| PMT | Programme Map Table |
| SW | Session Word |
| uimsbf | Unsigned Integer, Most Significant Bit First |

## 5 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 SW, such that only the intended parties will receive the transmission, outlined as follows:

1) The Session Word is entered at the DSNG unit in the field, or at the transmitting earthstation.
2) The Session Word is 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, then the broadcast is not received.

The security requirements for fixed contribution systems are somewhat different to the DSNG model. The secure exchange of SWs is fundamental to such systems and is achievable by encrypting them.

## 6 Modes of operation

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

– **Mode 0**: No scrambling.

– **Mode 1**: All components are scrambled by a fixed Control Word (CW), derived from a clear SW.

– **Mode E**: All components are scrambled by a fixed CW, derived from an Encrypted Session Word (ESW).

The scrambling mechanism, as defined in the DVB-CSA specification, shall be applied at the Transport level only.

A Conditional Access Table (CAT) shall be present in the multiplex for BISS Mode 1 and BISS-E, although the table shall be empty as no Entitlement Management Message (EMM) stream will be present.

NOTE – 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 E must also support Modes 0 and 1.

## 7 Mode 0

The Scrambler must be capable of disabling the scrambling operation. In this mode, there will be no *CA_descriptor* in the Programme Map Table (PMT) and no Entitlement Control Message (ECM) stream. The *Transport_Scrambling_Control* bits of the Transport Packets will be set to "00".

## 8 BISS Mode 1 – Functional requirements

### 8.1 Overview

This mode has been designed specifically for DSNG applications, fly-away operations, emergency situations, etc. It may also be used as a fall-back solution while using the complete BISS-E system. In Mode 1, a fixed 12-character SW is inserted in the scrambler. The 64-bit CW is derived from the SW according to the DVB-CSA specification.

Manual entry of the SW shall be in hexadecimal notation, 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 that interface is beyond the scope of this Recommendation.

The Scrambler shall ensure that the SW cannot be changed more than ten times in a 5-minute period and that there is a minimum of 10 seconds between changes.

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 BISS.

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

## 8.2 CA_descriptor

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

**Table 1/J.96 – 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 |
| } | | |

***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 BISS is `0x2600`. See [2].

**CA_PID**: This is a 13-bit field indicating the Packet Identification Number (PID) of the Transport Stream packets that shall contain the ECM information. For BISS, no ECM information is required, so this field shall contain the value `0x1FFF`.

# 9 BISS Mode E – Functional requirements

## 9.1 Clear Session Word

The unit shall be compliant with BISS Mode 1. It shall support the insertion of a 12-character clear SW through the front panel and through a remote control interface. It shall use the SW as specified in clause 8 (BISS Mode 1).

The clear SW, once entered via the user interface or remote control port, shall not be readable through any unit interface.

## 9.2 Encrypted Session Word

The unit shall support the insertion of ESWs through the front panel and through a remote control interface. The definition of the remote control port is outside the scope of this Recommendation.

The ESW is a 16-character number that is transformed by the unit into a 12-character clear SW. The clear SW is then used by the unit to decrypt the broadcast according to clause 8 (BISS Mode 1).

Once the ESW has been entered via the front panel or via the remote control interface, it shall be impossible to read it back through any unit interface.

The manual entry of the ESW shall be in hexadecimal form; the 16 digits are entered with the most-significant nibble first (i.e. the left-most nibble).

For example, if the ESW is `0xF76EE249BE01A286`, it shall be entered in the following sequence:

`F,7,6,E,E,2,4,9,B,E,0,1,A,2,8` and `6`

### 9.3 Decryption scheme

### 9.3.1 Overview

The equipment shall include the following features:

- an **identifier**, denoted ***ID***, comprising a 14-character hexadecimal word which shall be *injected* by the user and shall be used as the default. The injected ID is mandatory. Optionally, in addition, the supplier may *bury* an ID. In this case, the user shall actively select the buried ID.
- a **DES decryption function**, denoted ***f( )***, as described in 9.3.3. Additional functions may be supplied but are beyond the scope of this Recommendation.
- a **simple post-processing function**, denoted ***P( )***, as described in 9.3.4.

The processing of the ESW in the unit to provide the clear SW is illustrated in Figure 1. A detailed specification of the Data Encryption Standard (DES) is outside the scope of this Recommendation.

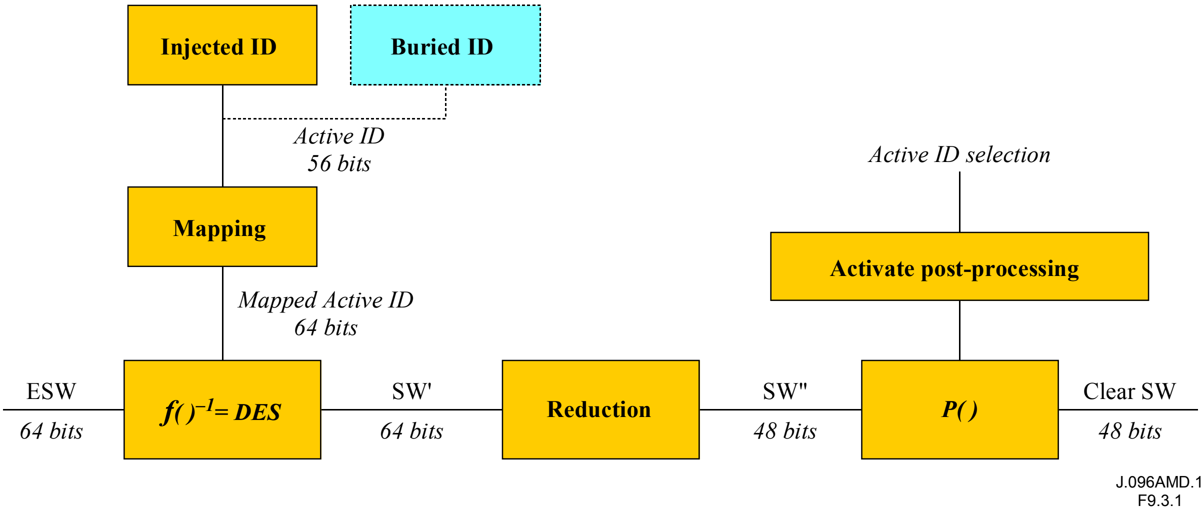

**Figure 1/J.96 – The signal processing required to produce a clear Session Word**

The mapping of the ID is a simple expansion from 56 to 64 bits, by adding an odd parity bit after every 7 bits. The reduction of the decrypted SW from 64 to 48 bits is obtained by deleting the first and last bit of each byte.

After the application of the post-processing function, ***P( )***, the clear SW is obtained to feed the BISS equipment as in Mode 1.

### 9.3.2 Unit identifiers

This Recommendation specifies two types of identifiers for each unit.

1) An **injected identifier** ($ID_i$) which is a secret key embedded in the unit. This is ***mandatory***.

2) Additionally, the manufacturer may provide a **buried identifier** ($ID_b$), defined by the manufacturer and linked uniquely to the device itself. This is not mandatory, but if implemented it shall comply with this Recommendation.

A user shall be able to select the identifier of his choice via the front panel and the remote control interface. The selected identifier is used as the active key to decrypt the ESW.

a) Injected ID – mandatory

The injected ID is a 14-character identifier that can be entered in the BISS unit by the user at any time.

Units shall support the insertion of the injected ID through its front panel and through its remote control interface. There shall be no mechanism for reading back part or all of the injected ID via any unit interface.

The same ID can be injected in more than one piece of equipment, e.g. for redundancy management.

The manual or remote entry of the injected ID shall be in hexadecimal form; the 14 digits are entered with the most-significant nibble first (i.e. the left-most nibble).

For example, if the injected ID is `0xF09A423F56738A`, it shall be entered in the following sequence:

`F,0,9,A,4,2,3,F,5,6,7,3,8` and `A`

b) Buried ID – optional for the supplier

The buried ID is a 14-character identifier that uniquely identifies a particular unit. Buried IDs are optional.

Two different units shall have a different buried ID, at least for the equipment produced by the same manufacturer. Units from different manufacturers could have the same buried ID, but that would be a fortuitous case.

The manufacturer shall ensure that, without his agreement, nobody can modify the buried ID.

### 9.3.3 Decryption function

Units shall implement the interoperable function specified in b) below. Additional decryption functions may optionally be implemented. In this case, it shall be possible to select the decryption function via the front panel and the remote control interface. The definition of these additional functions is outside the scope of this Recommendation.

The interoperable function is mandatory on all units. It uses the 64-bit ESW and the 64-bit Mapped Active ID to compute a 12-character word called SW".

a) *Mapping*

The Mapped Active ID is derived from the 56-bit Active ID by mapping the 56 Active ID bits into the upper seven bits of a sequence of 8 bytes, then the lsb of each byte is set such that the resultant byte has odd parity (see Table 2).

**Table 2/J.96 – Mapping of Active ID to Mapped Active ID**

| Active key bit | Mapped byte/bit | Mapped key bit |
|---|---|---|
| 55 | 0/7 | 63 |
| 54 | 0/6 | 62 |
| 53 | 0/5 | 61 |
| 52 | 0/4 | 60 |
| 51 | 0/3 | 59 |
| 50 | 0/2 | 58 |
| 49 | 0/1 | 57 |
| Odd_parity | 0/0 | 56 |
| 48 | 1/7 | 55 |
| Etc. | Etc. | Etc. |
| NOTE – The above uses engineering notation: msb = bit 63, lsb = bit 0. | | |

b) *Interoperable function*

The interoperable function is the simple DES algorithm used in the Electronic Codebook (ECB) mode and the decrypt state. This function is described in FIPS PUB 46-3 [3] and FIPS PUB 81 [4]. The algorithm key is the 64-bit Mapped Active ID[1]. The data bloc to decrypt is the ESW. Note that this Recommendation uses *engineering* notation (msb = bit 63, lsb = bit 0), while DES uses *FIPS* notation (msb = bit 1, lsb = bit 64). Hence the bit mapping is:

– DES key (1 ... 64) → Mapped Active ID (63 ... 0);

– DES data bloc (1 ... 64) → ESW (63 ... 0).

The result of the decryption algorithm is defined in 64 bits and is called SW'.

The mapping between SW' and SW" is given in Table 3. This mapping simply removes the most significant and the least-significant bit of each byte. The third column of the table is the DES result, where the bits are numbered using FIPS notation.

**Table 3/J.96 – Mapping between SW' and SW"**

| | | |
|---|---|---|
| SW"(47) | SW'(62) | D(2) |
| SW"(46) | SW'(61) | D(3) |
| SW"(45) | SW'(60) | D(4) |
| SW"(44) | SW'(59) | D(5) |
| SW"(43) | SW'(58) | D(6) |
| SW"(42) | SW'(57) | D(7) |
| SW"(41) | SW'(54) | D(10) |
| SW"(40) | SW'(53) | D(11) |
| SW"(39) | SW'(52) | D(12) |
| SW"(38) | SW'(51) | D(13) |
| SW"(37) | SW'(50) | D(14) |
| SW"(36) | SW'(49) | D(15) |
| SW"(35) | SW'(46) | D(18) |
| SW"(34) | SW'(45) | D(19) |
| SW"(33) | SW'(44) | D(20) |
| SW"(32) | SW'(43) | D(21) |
| SW"(31) | SW'(42) | D(22) |
| SW"(30) | SW'(41) | D(23) |
| SW"(29) | SW'(38) | D(26) |
| SW"(28) | SW'(37) | D(27) |
| SW"(27) | SW'(36) | D(28) |
| SW"(26) | SW'(35) | D(29) |
| SW"(25) | SW'(34) | D(30) |
| SW"(24) | SW'(33) | D(31) |

[1] The DES algorithm does not use bits 8, 16, 24, 32, 40, 48, 56 and 64 of the key, numbered with the FIPS notation. Hence the useful key length is actually 56 bits, which is compatible with the exportation restrictions.

**Table 3/J.96 – Mapping between SW' and SW"**

| | | |
|---|---|---|
| SW"(23) | SW'(30) | D(34) |
| SW"(22) | SW'(29) | D(35) |
| SW"(21) | SW'(28) | D(36) |
| SW"(20) | SW'(27) | D(37) |
| SW"(19) | SW'(26) | D(38) |
| SW"(18) | SW'(25) | D(39) |
| SW"(17) | SW'(22) | D(42) |
| SW"(16) | SW'(21) | D(43) |
| SW"(15) | SW'(20) | D(44) |
| SW"(14) | SW'(19) | D(45) |
| SW"(13) | SW'(18) | D(46) |
| SW"(12) | SW'(17) | D(47) |
| SW"(11) | SW'(14) | D(50) |
| SW"(10) | SW'(13) | D(51) |
| SW"(9) | SW'(12) | D(52) |
| SW"(8) | SW'(11) | D(53) |
| SW"(7) | SW'(10) | D(54) |
| SW"(6) | SW'(9) | D(55) |
| SW"(5) | SW'(6) | D(58) |
| SW"(4) | SW'(5) | D(59) |
| SW"(3) | SW'(4) | D(60) |
| SW"(2) | SW'(3) | D(61) |
| SW"(1) | SW'(2) | D(62) |
| SW"(0) | SW'(1) | D(63) |

### 9.3.4 Post-processing function

The post-processing function ***P( )*** converts SW" into the clear SW, as shown in the example below. The conversion gives different results, depending on the type of ID used to decrypt the ESW. When the active key is the **injected ID**, function ***P( )*** is the **identity function** (i.e. SW" = SW). If the optional **buried ID** is used, function ***P( )*** consists of **rotating** the SW" by **one bit to the right**.

If SW" = b47 b46 ... b1 b0

$$\text{SW} = \boldsymbol{P}(\text{SW}'') = \begin{cases} \text{b47 b46 ... b1 b0} & \text{If the active key is an } \textbf{injected ID} \\ \text{b0 b47 b46 ... b2b1} & \text{If the active key is a } \textbf{buried ID} \\ \text{Undefined} & \textbf{Other} \text{ cases} \end{cases}$$

In **other** cases, the definition of ***P( )*** is outside the scope of this Recommendation. It shall however have a different mathematical behaviour (i.e. it shall produce different results) than when the active key is either the *injected* ID or the *buried* ID.

# Bibliography

[1] *DVB Common Scrambling Algorithm*, V. 2.0. (July 2002).
http://portal.etsi.org/dvbandca/DVB/DVBINTRO.asp

[2] ETSI ETR 289 (1996), Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems.
http://webapp.etsi.org/workprogram/SimpleSearch/QueryForm.asp

[3] FIPS PUB 46-3 (1999), *Data Encryption Standard*.
http://www.itl.nist.gov/fipspubs/by-num.htm

[4] FIPS PUB 81 (1980), *DES Modes of Operation*.
http://www.itl.nist.gov/fipspubs/by-num.htm

# SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series B | Means of expression: definitions, symbols, classification |
| Series C | General telecommunication statistics |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| **Series J** | **Cable networks and transmission of television, sound programme and other multimedia signals** |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks and open system communications |
| Series Y | Global information infrastructure and Internet protocol aspects |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2002