INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.96

(03/2001)

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 J.89

ITU-T Recommendation J.96

(Formerly CCITT Recommendation)

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 J.89

Summary

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).

Practical implementations are also provided in Annex A.

Source

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

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 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).

Practical implementations are also provided in Annex A.

2 References

2.1 Normative reference

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T H.222.0 (2000) | ISO/IEC 13818-1:2000, *Information technology – Generic coding of moving pictures and associated audio information*: *Systems*.

[2] ETSI ETR 162 (1995), *Digital Video Broadcasting (DVB); Allocation of Service Information (SI) codes for DVB systems*.

[3] ETSI ETR 289 (1996), *Digital Video Broadcasting (DVB); Support for use of scrambling and conditional access (CA) within digital broadcasting systems*.

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

[5] ITU-T J.81 (1993), *Transmission of component-coded digital television signals for contribution-quality applications at the third hierarchical level of ITU-T G.702*.

[6] ITU-T J.89 (1999), *Transport Mechanism for component-coded digital television signals using MPEG-2 4:2:2 P@ML including all service elements for contribution and primary distribution*.

[7] EBU Tech3290 (2000), *Basic Interoperable Scrambling System (BISS)*.

2.2 Bibliographic reference

– OKAPI: BOUCQUEAU (J.M.), SERRET (J.), QUISQUATER (J.J.) and MACQ (B.): *Security in Multimedia Teleservices in Multimedia Telecommunications Services; Cost 237 – Final Report, Springer, September 1999, pp. 348-373*.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 scrambling: The alteration of the characteristics of a vision/sound/data signal in order to prevent unauthorized reception in a clear form. This alteration is a specified process under the control of the conditional access system (sending end).

3.2 descrambling: The restoration of the characteristics of a vision/sound/data signal in order to allow reception in a clear form. This restoration is a specified process under the control of the conditional access system (receiving end).

4 Abbreviations

This Recommendation uses the following abbreviations:

3DES	Triple DES
ABC	DES Keys A, B, C
ACS	Access Control System
Bit	A contraction of the words "binary digit"
bslbf	Bit String, Left Bit First
CA	Conditional Access
CAT	Conditional Access Table
CD	Controller Device
CK	Common Key
CSA	Common Scrambling Algorithm
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
MD	Manager Device
MH	Message Header
msb	Most Significant Bit
MSB	Most Significant Byte
NMC	Network Management Centre
OKAPI	Open Kernel for Access to Protected Interoperable interactive Services
Octet	A sequence of 8 bits operated on as a data group or word

PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
PMT	Program Map Table
PRG	Pseudo-Random (sequence) Generator
PSI	Program Specific Information
PSPN	Public Switched Packet Network
PSTN	Public Switched Telephone Network
SAM	Scrambling Authorization Module
SK	Session Key
SM	Security Module
SNG	Satellite News Gathering
SW	Session Word
TTP	Trusted Third Party
uimsbf	Unsigned Integer, Most Significant Bit First
Word	A group or sequence of bits treated together

5 System overview

ITU-T J.89, which defines the transport mechanism for component-coded digital television signals using MPEG-2 4:2:2P@ML including all service elements, is now widely used for contribution and primary distribution and also for SNG applications as in ITU-R SNG.1421.

A conditional access system, needed to ensure privacy in long-distance international television transmission, is used to enable authorized users to descramble the components of a service. In addition, for SNG applications a simplified system based on a fixed key may be required.

The information required for descrambling may be either manually introduced in the decoder (by a fixed local "control word" as in part A of Figure 1, by pre-stored variable local control words accessed through a password or a session key (part B of Figure 1) or provided by the conditional access system summarized in part C of Figure 1).

Figure 1 illustrates the scrambling processes.

This Recommendation uses the DVB Common Scrambling Algorithm (CSA) including the modification for DSNG applications. In order to use the algorithm, a non-disclosure agreement must be signed with ETSI, including payment of a one-time royalty (for details, go to www.etsi.org and click on **Security algorithms and codes** under the heading **Publication and Products**.

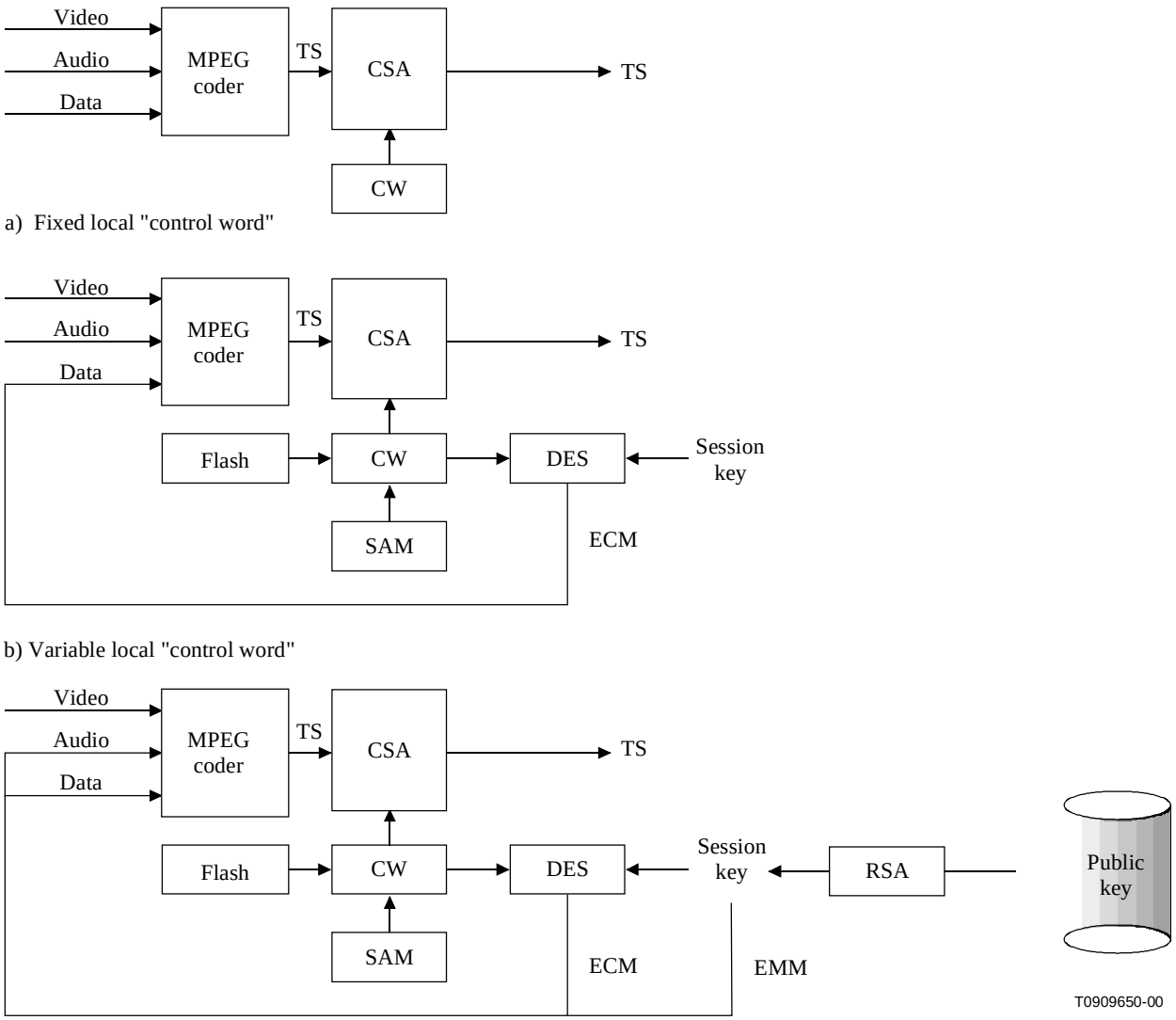


Figure 1/J.96 – General description of the scrambling/descrambling processes

The three implementations illustrated in Figure 1 are described in Annexes A and B.

6 Application in the MPEG/DVB environment

Scrambling

Scrambling is a process used to make an information incomprehensible for unauthorized receivers during transmission of this information.

The CSA uses common keys to initialize the scrambling_descrambling process at each transport packet. These common keys are issued from control words (CW) that are sent in the stream.

Scrambling can be done at transport or PES packets level.

Control words can evolve in time, with a duration named "crypto-period". In order to synchronize the receivers, they are designated as "odd CW" or "even CW". Each scrambled packet indicates, by use of "transport_scambling_control" bits, if it is scrambled or not and the parity of the current CW. Crypto-period can vary from some seconds (major CAS) to the duration of a complete transmission ("fixed control word" for DSNG).

Conditional access

Conditional access system (CAS) consists of tools that enable the authorized receivers to obtain control words in order to descramble information.

These tools are typically Entitlement Control Messages (ECM) and Entitlement Management Messages (EMM) which are broadcast in the transport stream. Syntax of private part of ECM and EMM depends on the CAS.

ECM typically contains a cryptogram of CWs and access criteria. Their contents vary with a period equal to the crypto-period.

For DSNG, if the CW is a constant for one transmission, ECM can be replaced by any out-of-band medium to specify which CW will be used during the whole transmission.

6.1 MPEG and ETR 289 specifications

6.1.1 Scrambling

MPEG has defined the Transport_Scrambling_Control bits of transport packet headers. ETR 289 [3] has specified these bits as shown in Table 1.

Table 1/J.96 – Transport_scrambling_control values

Value	Description
00	Not scrambling of TS packet payload
01	Reserved for future DVB use
10	TS packet scrambled with Even Key
11	TS packet scrambled with Odd Key

NOTE – In Europe, all the CAS have to use this algorithm (available at ETSI as custodian, under NDA – non-disclosure agreement).

6.1.2 PSI/SI

ISO has defined a PID = 0x01 which is reserved to the Conditional Access Table. Its contents is used by receiver to find EMM PIDS.

The CAT syntax is given in Table 2 (Table 2-27 in [1]).

Table 2/J.96 – Conditional access table

Syntax	No. of bits	Mnemonic
CA_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
reserved	**18**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
CRC_32	**32**	**rpchof**
}		

The CA_Descriptor syntax is given in Table 3 (Table 2-51 in [1]).

Table 3/J.96 – Conditional access descriptor

Syntax	No. of bits	Mnemonic
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
for (i = 0; i < N; i++) {		
private_data_byte	**8**	**uimsbf**
}		
}		

ISO has defined the Program Map Table (PMT) in which CA_Descriptors may be used by receivers to find ECM PIDS. See Table 4 (Table 2-28 in [1]).

Table 4/J.96 – Program map table

Syntax	No. of bits	Mnemonic
TS_program_map_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
program_number	**16**	**uimsbf**
reserved	**2**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
reserved	**3**	**bslbf**
PCR_PID	**13**	**uimsbf**
reserved	**4**	**bslbf**
program_info_length	**12**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
for (i = 0; i < N1; i++) {		
stream_type	**8**	**uimsbf**
reserved	**3**	**bslbf**
elementary_PID	**13**	**uimsnf**
reserved	**4**	**bslbf**
ES_info_length	**12**	**uimsbf**
for (i = 0; i < N2; i++) {		
descriptor()		
}		
}		
CRC_32	**32**	**rpchof**
}		

EN 300 468 [4] has specified a free_CA_mode bit in Service Description Table (SDT) and Event Information Table (EIT). This bit has to be set when access to at least one component is controlled by a CA_System (see 5.2.4 in [4]).

6.1.3 Conditional access messages

The syntax for CA message table and specified Table_Id values are given in Tables 5 and 6 (Tables 3 and 4, respectively, in [4]). CA_section_length value is limited to 253 (max section size = 256 bytes).

Table 5/J.96 – 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**
}		
}		

Table 6/J.96 – 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

6.2 DSNG specifications

The following is based on the four modes as defined in ITU-T J.81:

– mode 0: No scrambling;

– mode 1: Components are scrambled by a single fixed CW;

– mode 2: All components of the programme are scrambled by a unique CW;

– mode 3: Components are scrambled by more than one CW.

A CA_System_Id has to be delivered by ETSI with value in the range 0x1 to 0xff (standardized CA systems) according to [2].

In modes 1 to 3, scrambling will be applied at TS level.

In all modes, ECM and/or EMM, if present, will be compliant with [3], concerning maximum section length of 256 bytes, section syntax and table_id values.

6.2.1 Mode 0

There is no scrambling. The two Transport_Scrambling_Control bits are zeroed.

A CAT and EMM stream may be present if needed to transmit rights for programmes scheduled in mode 1 to 3 (contents to be defined).

No CA_descriptors in PMT. No ECM in the stream.

6.2.2 Mode 1

The first Transport_Scrambling_Control bit is set. The second one may vary at event boundaries during the transmission. The CW used belong to a list of control words present in scrambling and descrambling equipment.

A CAT and EMM stream may be present if needed.

One CA_descriptor is present in PMT at program level. An example is given below:

Syntax	No. of bits	Mnemonic
CA_descriptor() {		
descriptor_tag = 0x09	**8**	**uimsbf**
descriptor_length = 0x07	**8**	**uimsbf**
CA_system_ID = 0x0001 to 0x00ff (t.b.d)	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID = dummy value	**13**	**uimsbf**
Mode_id = 0x01	**8**	**uimsbf**
Odd_CW_index	**8**	**uimsbf**
Even_CW_index	**8**	**uimsbf**
}		

Mode_id = 0x01 indicates to the receiver that it does not need to receive any ECM (in this mode, no ECM stream is present, CA_PID has a dummy value) and that following bytes give CW_index.

Odd_CW_index and Even_CW_index are used to select a CW in the list of CWs stored in the receiver.

Any change of CW_index value will be signalled by a new version number in the PMT. Correct handling of odd and even CWs may allow to "change" the "fixed" CW at event boundaries with seamless transitions or to change a list of CW in receiver and scrambler (current list, next list).

6.2.3 Modes 2 and 3

The first Transport_Scrambling_Control bit is set. The second one is varying during the transmission and indicates to the descrambler which CW is in use (odd or even).

A CAT and EMM stream may be present if needed.

One CA_descriptor may be present in PMT at program level, giving an ECM_pid for all components of the program. Additional CA_descriptors may be present at component level. In this case, it supersedes the value which has been specified at program level, only for the concerned component.

Example 1: mode 2, all components scrambled with CW1:

– either one CA_Desc at program level with ECM_PID_1, or

– one CA_Desc at component level with ECM_PID_1 for each component.

Example 2: mode 3, video and sound 1 scrambled with CW1, sound 2 with CW2 and sound 3 with CW3:

– one CA_Desc at program level with ECM_PID_1, and
– one CA_Desc at audio 2 level with ECM_PID_2, and
– one CA_Desc at audio 3 level with ECM_PID_3.

6.2.4 Summary

The table below summarizes the present items during one transmission:

Item	Mode 0	Mode 1	Mode 2	Mode 3
Transport_Scrambling_Control	**00**	**Constant 10 or 11**	**Alternating 10/11**	**Alternating 10/11**
CAT	**Optional**	**Optional**	**Optional**	**Optional**
EMM	**Optional**	**Optional**	**Optional**	**Optional**
CA_Descriptor(s) in PMT	**No**	**Yes**	**Yes**	**Yes**
ECM	**No**	**No**	**Yes**	**Yes**

ANNEX A

Practical implementation permitting interoperability

A.1 Introduction

A.1.1 Overview

This annex proposes the additional mechanisms required for conditional access to allow interoperability of DSNG vendors equipment.

Only mode 1 (fixed Control Word Scrambling) is mandatory.

A.1.2 Nomenclature

Throughout this annex, the term "Scrambler" relates to the overall mechanisms required to meet the CSA specification.

Throughout this annex, the term "Scrambling Module" relates to the Super Scrambling Mechanisms required to meet the CSA specification.

NOTE – In order to obtain the CSA specification, a non-disclosure agreement must be signed with ETSI, including payment of a one-time royalty (for details, go to www.etsi.org and click on **security algorithms and codes** under the **Publication and Products** heading).

Throughout this annex, the term "SAM" relates to the Scrambling Authorization Module as required to meet the CSA specification.

Throughout this annex, 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 to scramble the transport stream directly or adding a level of indirection, a key used to scramble changing CWs within Entitlement Control Messages.

Throughout this annex, 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.

A.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.

NOTE – In order to obtain the CSA specification, a non-disclosure agreement must be signed with ETSI, including payment of a one-time royalty (for details, go to www.etsi.org and click on **Security algorithms and codes** under the **Publication and Products** heading).

A.2 Functional requirements

A.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 CSA specification. 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 Recommendation; 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 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.

A.2.2 Mode 0

The Scrambler must be capable of disabling 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".

A.2.3 Mode 1

A.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 CSA specification, respectively. An overview is given in Figure A.1.

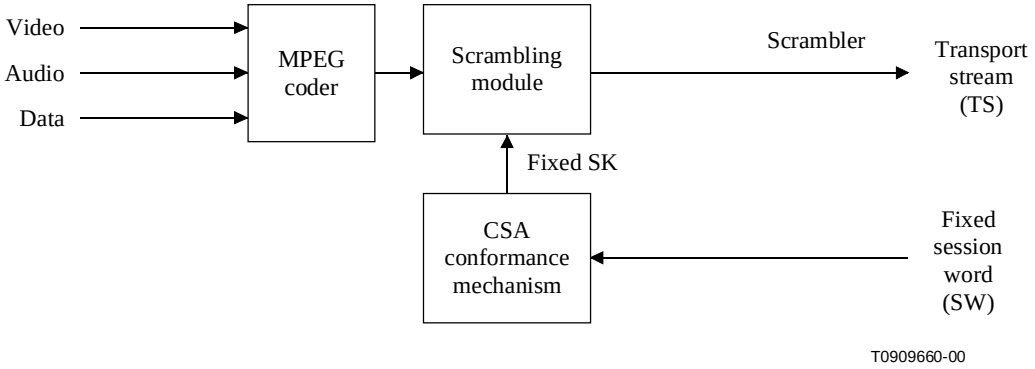


Figure A.1/J.96 – Overview: Mode 1

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 CSA specification.

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

Table A.1/J.96 – 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)	(Note 1)
CW(5)	SW(4)
CW(6)	SW(5)
CW(7)	SW(6)
CW(8)	(Note 2)
NOTE 1 – CW(4) is derived from SW(1)..SW(6) by the CSA Conformance Mechanism.	
NOTE 2 – CW(8) is derived from SW(1)..SW(6) by the CSA Conformance Mechanism.	

In this mode there will be a CA_descriptor in the PMT, present at program 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.

E.g., 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 Recommendation.

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.

A.2.3.2 CA descriptor

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

Table A.2/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 mode 1 is 0x2600 [2].

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.

A.2.4 Modes 2 and 3

A.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 Figure A.2.

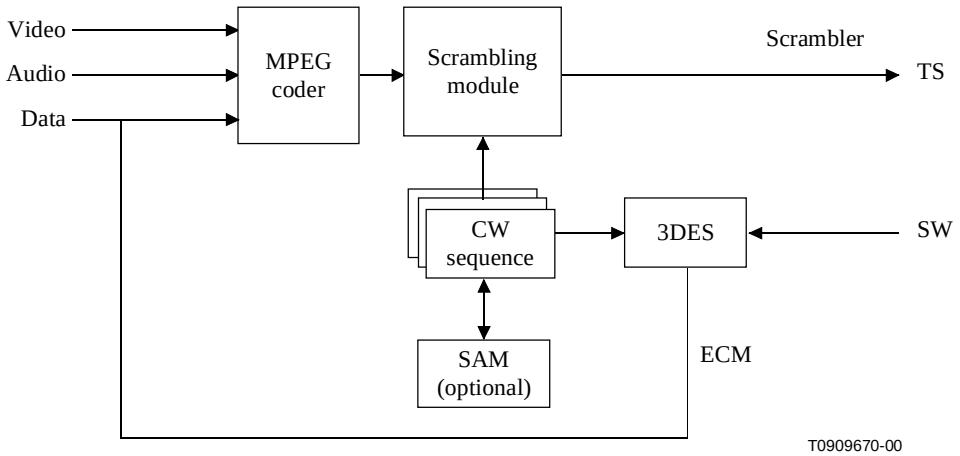


Figure A.2/J.96 – Overview: Modes 2 and 3

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 in 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 program 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 (see Note). 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.

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

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.

A.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 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 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 = 0x00000000000000000000000000011223344556677.

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

Table A.3/J.96 – 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 Recommendation. However, to allow for true interoperability, a KE value of "00000000000000000000000000000000" is assigned for fixed_bits_option = "0x00" (default).

The bit mapping between the CW and the 3DES cypher block is shown in Table A.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 A.4/J.96 – 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)

A.2.4.3 Entitlement Control Message

The ECM is in the form of a section as defined by ITU-T H.222.0 | ISO/IEC 13818-1 [1]. The message format for an ECM, as part of this Recommendation, is given in Table A.5.

Table A.5/J.96 – 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, 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 attack of the ECM stream is much easier. To achieve a proper balance the repetition rate of ECMs shall be 10/s 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.

A.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 A.6.

Table A.6/J.96 – 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.

APPENDIX I

General description of an open conditional access system based on OKAPI

The access to the control of the scrambling sequence is secured by using the Public Key Infrastructure (PKI), which is an open system for cryptographic applications.

I.1 Public key crypto-systems

The notion of public key cryptography was introduced by Diffie and Hellman. Public key systems differ from conventional systems in that there is no longer a single secret shared by a pair of users. Rather, each user has his own key material. Furthermore, the key material of each user is divided into two portions: a private component and a public component. The public component generates a public transformation *E*, and the private component generates a private transformation *D*. In analogy to the conventional case, *E* and *D* might be termed encryption and decryption functions respectively. However, this is imprecise: In a given system we may have *D(E(M)) = M*, *E(D(M)) = M*, or both.

A requirement is that *E* must be a trapdoor one-way function. One way refers to the fact that *E* should be easy to compute from the public key material but hard to invert unless one possesses the corresponding *D*, or equivalently, the private key material generating *D*. The private component thus yields a "trapdoor" which makes the problem of inverting *E* seem difficult from the point of view of the cryptanalyst, but easy for the (sole legitimate) possessor of *D*. For example, trapdoor may be the knowledge of the factorization of an integer.

We remark that the trapdoor functions employed as public transformation in public key systems are only a subclass of the class of one-way functions.

We note also that public/private dichotomy of *E* and *D* in public systems has no analogue in a conventional cryptosystem: In the latter, both E_k and D_k are parameterized by a single key *k*. Hence if E_k is known then it may be assumed that *K* has been compromised, whence it may also be assumed that D_k is also known, or vice versa. For example, in DES, both *E* and *D* are computed essentially by the same public algorithm from a common key; so *E* and *D* are both known or unknown, depending on whether the key has been compromised.

Public key cryptosystems offer at least the same security as the secret key ones. Their main drawback is the computation time, around 1000 times higher. But such a system presents a major advantage, the easiness of the key management system.

Regardless of whether a conventional or public key cryptosystem is used, it is necessary for users to obtain other users' keys. In a sense, this creates a circular problem: to communicate securely over insecure channels, users must first exchange key information. If no alternative to the insecure channel exists, then secure exchange of key information presents essentially the same security problem as subsequent secure communication.

In conventional cryptosystems, this circle can be broken in several ways. For example, it might be assumed that two users could communicate over a supplementary secure channel, such as a courier service. In this case it is often the case that the secure channel is costly, inconvenient, low-bandwidth and slow; furthermore, use of a courier cannot be considered truly secure. An alternative is for the two users to exchange key information via a central authority. Use of a central authority has several disadvantages.

In public key systems, the key management problem is simpler because of the public nature of the key material exchanged between users, or between a user and a central authority. Also, alternatives to the insecure channel may be simpler; for example, a physical mail system might suffice, particularly if redundant information is sent via the insecure (electronic) channel. Nevertheless, the most efficient way to manage keys in an asymmetric cryptosystem is through a certification scheme.

I.2 Certificate technology

One of the first issues that arise when designing a public-key-based protocol is its certificate architecture.

A new certificate technology, SPKI, has been recently designed within the IETF.

SPKI certificates are *key*-centred authorization certificates. They do not express a binding between a name and a key, but on the contrary, they directly express an authorization delegation over a public key. In the SPKI terminology, public keys are called "Principals". A principal is an entity that can express some authority by signing or/and deciphering some information. A principal also acts as a universal unique name for it, but to simplify and reduce the amount of data processed, the secure hashing of a principal is also admitted as its unique identifier.

Although SPKI also supports identity certificates, OKAPI only makes use of the authority certificates. SPKI authority certificates are initially issued by the verifying entity. The exact authority delegated can be easily fine-tuned with meaningful verifier defined free-text tags.

To give the system some flexibility, the authority delegated to a principal can be re-delegated by it to another principal. To enable this mechanism, the field "propagate" must be added to the original certificate. SPKI certificates are thought not to be unique (in the sense that they will express all the information needed by all the entities), and ideally a different certificate must be issued to cover each of the delegated authorities.

When an entity (the prover) wants to prove some authority to a verifier, it is its responsibility to provide all the certificates that the verifier will need. It is also required that the prover ordered them in such a way that if a certificate from another certificate needs to be validated this one has already been processed. At the end, the verifier will reduce the certificate chain to one certificate of the form:

(Issuer = self, Subject = prover, Authority = X, some time constraint).

SPKI introduces two new methodologies to deal with the certificate revocation issue: the online verification[1] and the certificate revalidation certificate (CRC). On the first one, the verifier is forced to contact the issuer (or a third entity) each time the certificate must be verified. On the second one, the prover is forced to contact the issuer (or a third entity) to obtain a CRC, and then forward the CRC and the original certificate to the verifier. Of course, the CRC also has a validity period.

OKAPI decided to use the revalidation method because it has the following advantages:

- No need to publish long CRLs.
- There is no need to contact the issuer for each verification. Once a CRC is obtained it can be used until it gets timed out.
- Revalidation certificate time to live is easy to adjust.
- The issuing of the certificate revalidation certificate can be strictly controlled. They are to be provided only to the principal owner of the original certificate.

SPKI made an Internet philosophy approach to the problem with data representation. SPKI certificates are represented by canonical S-expressions [4]. S-expressions are simple, easy to parse and human readable (up to some extent). S-expressions also represent very little overhead to the real data they contain. Extracted from the SPKI IETF draft: "*We define a canonical S-expression as containing binary byte strings each with a given length and punctuation "()[]" for forming lists. The length of a byte string is a non-negative ASCII decimal number, with no unnecessary leading "0" digits, terminated by ":". We further require that there be no empty lists and that the first list element be a byte string (as defined below). This form is a unique representation of an S-expression and is used as the input to all hash and signature functions.*" Of course, S-expressions can also be used for storage and transmission purposes. To help the reader understanding and illustrate the S-expressions simplicity hereunder are some examples of valid canonical S-expressions (between quotes):

- "(10:not-before19:1998-01-19_17:00:00)"
- "(11:hello world)"
- "(4:this(2:is(1:a(5:valid)(12:s-expression))))"

I.3 Practical operation with OKAPI

I.3.1 Introduction

There are two kinds of sites:

– The Network Management Centre includes one Control Device and one Management Device.

– Each Communication Site includes one or several Conditional Access Devices.

The Network Management Centre is unique for a network. It is responsible for management of network resources, allocation of available channels (a direct link between the planning (TPP) and the CAS management is proposed), synchronization between transmitters and receivers. The NMC might easily extend its responsibilities to new services such as fingerprinting through watermarking.

There are several Communication Sites. Each one could, at the same time, transmit and/or receive one or more scrambled TV programmes. In each such site, there is at least one Conditional Access Device that manages several transmitters and several receivers.

A third kind of site might be considered. The system requires a Certification Authority for the smart card customization. For security reasons, this off-line dedicated system might be located outside the NMC.

---

[1] One-time revalidation in SPKI's nomenclature.

The main features of the system are:

– a centralized management of the TV programme exchanges;
– an ability to select/authorize receivers very quickly, almost in real time;
– a simple Man-Machine Interface at the Network Management Centre and at the Communication Sites;
– no need of permanent connection between the Network Management Centre and the Communication Sites;
– a very high protection against piracy of the TV programmes transmitted via open networks such as satellites;
– a large range of opportunities for new services relying on the CAS security features;
– a series of mode allowing a high protection level, even with limited means on site.

Moreover, Communication Sites not directly connected to the Network Management Centre are nonetheless able to transmit and/or receive scrambled TV programmes.

In Figure I.1 and in the subsequent clauses, the Network Management Centre is currently abbreviated as NMC and the Conditional Access Devices as CADs.

A smart card in the Network Management Centre is optional.

One or more smart cards are used for transmitting and for receiving at each Communication Site.

An important clarification must be done between transmissions and programmes.

A transmission is characterized by:

– a satellite or other communication channel;
– one Communication Site used as a transmitter;
– one or more Communication Sites used as receiver(s);
– a start and end date and time;
– a set of TV components including sound(s), vision and data.

A programme is characterized by:

– one programme name;
– one or more transmissions;
– one authorization key;
– one or more access criteria.

Consequently, one transmission can be used for broadcasting one or more programmes and one programme can be transmitted through one or more transmissions.

Three different behaviours are considered:

– the behaviour of the Network Management Centre;
– the behaviour of the transmitter of a Communication Site when using one of its encoders;
– the behaviour of the receiver of a Communication Site when using one of its decoders.

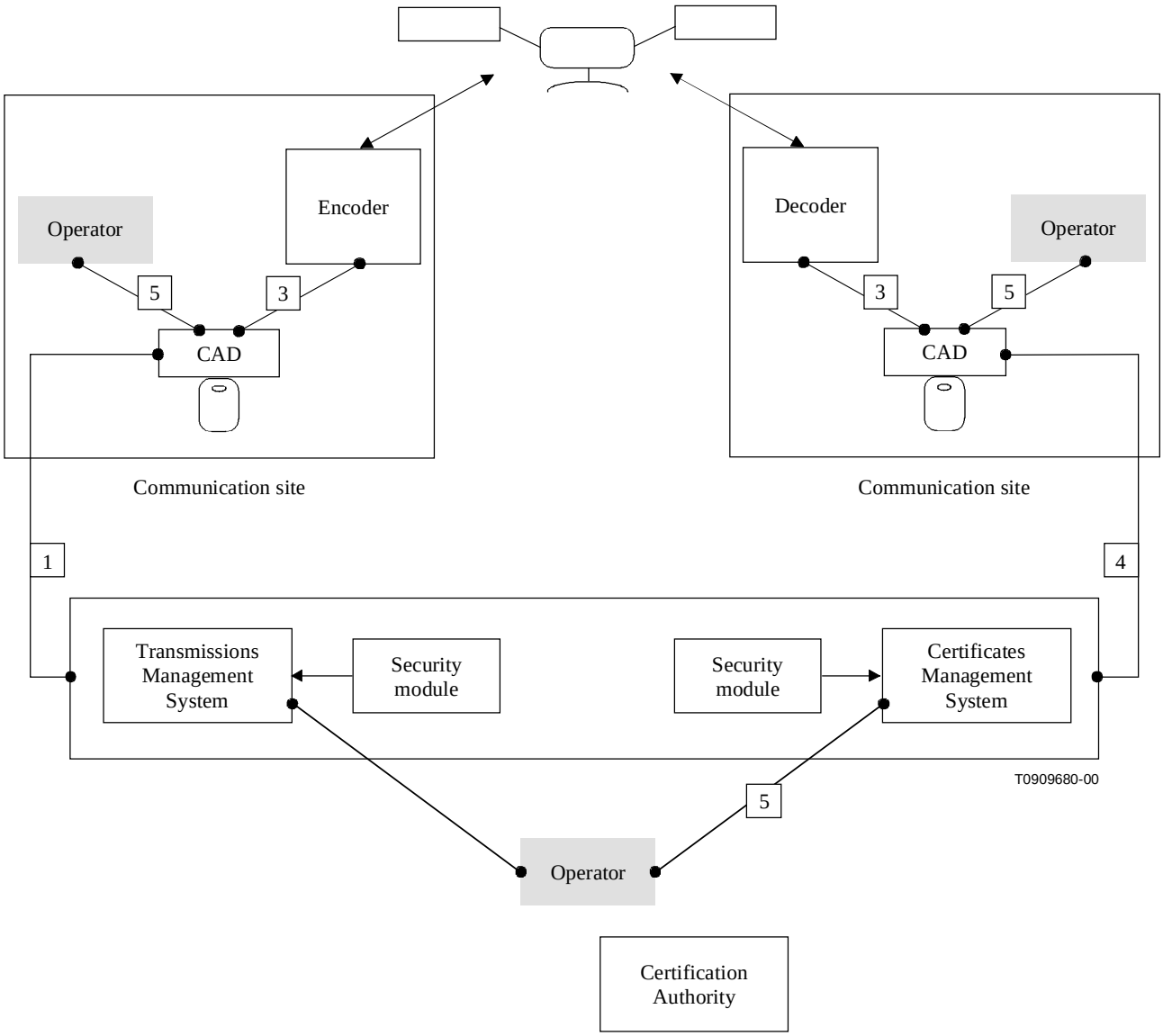


Figure I.1/J.96 – Architecture of the network

I.3.2 Functionality of the Network Management Centre

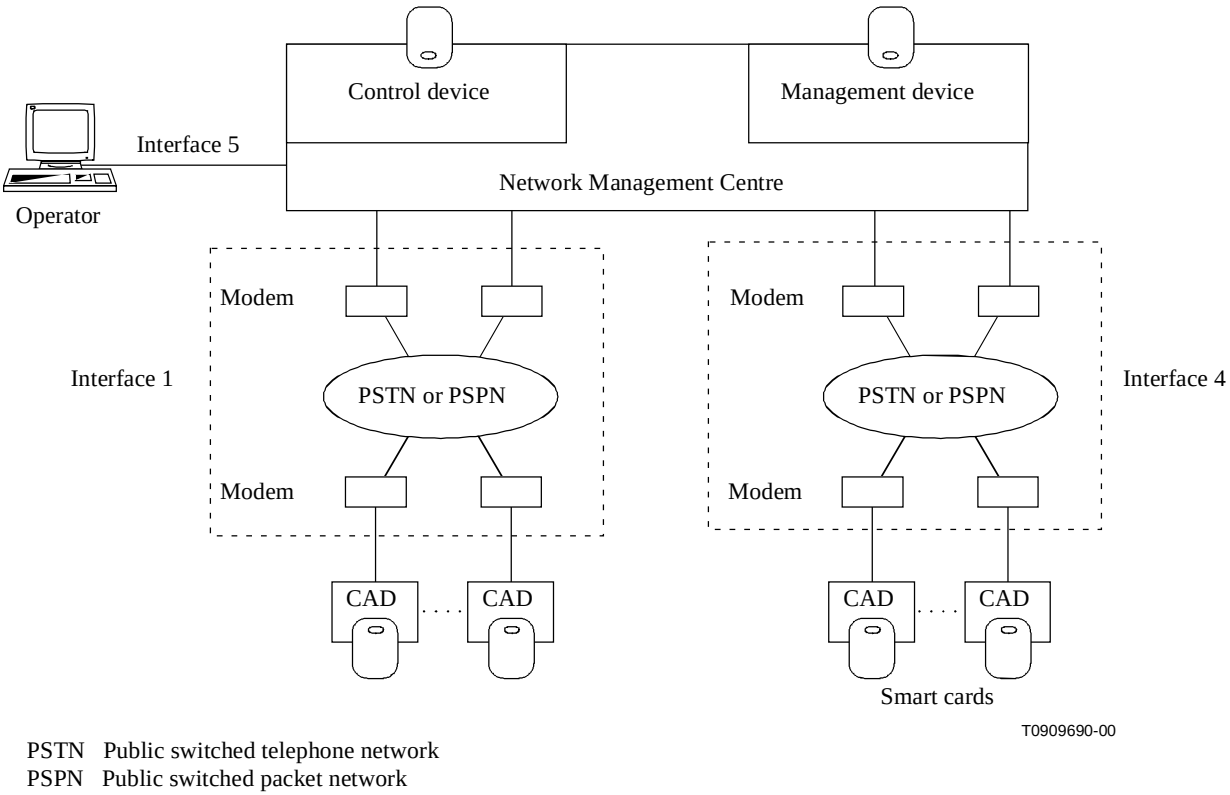
It is the responsibility of the NMC to ensure that the transmitter and all the authorized receivers get the correct authorization key and the correct access entitlements before the transmission of the programme. It is also the responsibility of the NMC to regularly update the authorization keys for security reasons. To do this, the NMC builds and sends ECMs and EMMs.

The NMC also ensures the supervision of all these smart cards, through its role of TTP.

The NMC manages a public key directory; solutions such as ITU-T X.500 | ISO/IEC 9594-1 might be considered in the future.

The NMC is responsible for the decision on the applied scenario (bidirectional procedure, unidirectional procedure, tokens, and local control word).

Figure I.2 gives a schematic of a NMC.



PSTN Public switched telephone network
PSPN Public switched packet network

Figure I.2/J.96 – Network Management Centre (NMC)

I.3.2.1 ECM generation

The NMC has to generate the ECMs. For that, the NMC generates control words, enciphers those control words eventually using a smart card and creates the corresponding ECMs. Each ECM is protected by a cryptographic checksum computed by cryptographic means. During the transmission, a new ECM is sent regularly. The ECMs are sent to the CAD of the transmitter through the interface 1.

One immediate way of implementing the scheme is to regularly create ECMs and to send them "online" to the CAD of the transmitter. Such an implementation supposes that during the whole transmission, the NMC remains connected to the CAD of the transmitter. Besides, the NMC, which drives all the transmitters, would have to generate several sets of ECMs (as many as there are channels in operation at that time) and to send them at the same time.

The use of ECM cyclic files removes such a constraint. Those files contain as many ECMs as needed for the estimated duration of the transmission. If the transmission were to overrun, the last ECM is built in such a way that it can be followed by the first ECM of the same file, in order to be able to loop through the same set of ECMs.

The NMC could generate a pool of ECM cyclic files before any identified need and send them to the CAD in advance, or at the last moment before a transmission.

Sending several ECM cyclic files in advance to the CAD will make it ready to operate almost immediately, even in the case of impulsive (last-minute planned) TV transmissions or in the case of an isolated transportable transmitter.

The most innovative aspect in the OKAPI CAS resides in the EMMs for which PKI facilities are fully exploited. In accordance with DSNG219, the protection of the transmission through a unique EMM and no ECM should be considered.

It should be stressed that the proposed system would gain in efficiency by intimately linking the transmission planning and protection.

I.3.2.2 EMM generation

The NMC also has to generate the EMMs for distributing keys and entitlements to specified smart cards.

One EMM is for the transmitter: it will allow the CAD of the transmitter (with the help of its smart card) to decipher the control word of all the above ECMs.

The other EMMs are for the receivers. They will allow authorized smart cards of the CADs of the receivers to decipher the control word of the above ECMs. There are two different ways of transmitting the EMMs:

– they can be transmitted directly using interface 4 (via phone, X.25, VSAT, direct connection) to the concerned CAD of each receiver;
– they can be broadcast to all the receivers via the transmitter encoder and the satellite channel.

EMMs can be generated in advance and stored either locally either remotely in the smart cards. It corresponds to the tokens scenario.

I.3.2.3 Supervision of smart cards and associated certificates

The NMC manages the contents of each smart card, eventually with the support of an external authority if the CA is delocated.

If impulse pay-per-view is used, then the NMC surveys the purchases of the smart cards.

The NMC has a database to know the contents of all smart cards and detailed information about all CADs (locations, smart cards' public key, etc.). The private key associate to each smart card MIGHT be known at this level.

If a smart card has no memory left, the NMC has to clean the memory by removing the obsolete keys and the obsolete entitlements.

I.3.2.4 Smart card issuing

The NMC generates issuing scenarios (description of all the keys and parameters to be written in each card) on request of its operator. Those scenarios are sent to an issuing tool, which initializes cards. The issuing tool sends back to the NMC a set of cards and a report file. The report file is used to update the database of the NMC. A certification authority ensures the smart cart issuing. It corresponds to a dedicated PC physically secured. This Certification Authority MIGHT be located in the NMC.

I.3.2.5 Man-Machine Interface

The Man-Machine Interface should consist of:

– a request of transmission;
– a description of all the transmission references described above;
– a consultation and an update of the database;
– a periodical survey of the cards configured for impulse pay-per-view;
– a journal of the alarms (a smart card is full or out of order; there are connection problems with a CAD).

At the NMC, the MMI should be developed with the concerned persons. Several logs to rapidly identify any trouble should be accessible.

I.3.3 Implementation of the CADs

The behaviour of the CAD of the transmitter consists of:

– maintaining the link with the NMC (e.g., regular pings to the NMC server);

– authenticate (first level) the EMMs sender;

– transmitting the relevant EMM(s) to its smart card(s) in order to store new key(s) and entitlement(s);

– regularly transmitting one ECM to its smart card to get back the corresponding CW that should be given to the encoder to scramble the TV programme;

– regularly transmitting to the encoder one ECM to broadcast to the decoders;

– if needed, transmitting also the EMMs to the encoder to send to the decoders.

The behaviour of the CAD of the receiver consists of:

– maintaining the link with the NMC (e.g., regular pings to the NMC server);

– authenticate (first level) the EMMs sender;

– getting the relevant EMMs from the decoder or from the direct link with the NMC and transmitting it to its smart card(s) in order to store new key(s) and entitlement(s);

– regularly getting the ECMs from the decoder and sending them to its smart card to get back the corresponding control words, and to give back to the decoder these control words.

I.3.3.1 Isolated transmitter station case

"Isolated" means that there is no connection between the CAD of the transmitter and the NMC at the moment of the transmission. This could be the case, for example, for a special news-reporting unit where the transmitter station is highly mobile. Any transmitter should be able to work in this mode in case of emergency.

In this context, it is still possible to secure the TV programme transmission. To make it possible, the CAD of the transmitter must be loaded in advance (using a diskette, a PCMCIA memory card or the smart card itself) with an ECM cyclic file. The only thing to do then for the operator of the transmitter is to select the appropriate ECM cyclic file.

In case of transmission involving both connected and isolated stations, the tokens scenario should be applied. This scenario is under patent process.

This mode is very appropriate when using impulse pay-per-view. The smart cards of the receivers will automatically store the number of the programme (with the agreement of the receiver operator). The NMC will later on survey the content of the cards.

I.3.4 Implementation of the interface 1

The interface 1 connects the NMC to the CAD of the transmitter. It is initialized by the NMC.

The following messages and commands are exchanged:

– ECMs: The recommended implementation consists of an ECM cyclic file that is computed by the NMC and transmitted in advance to the CAD of the transmitter together with the reference of the TV programme that will use those ECMs. Another implementation would consist in sending one ECM "online" every 8.2 seconds.

– EMMs: The recommended implementation consists of an EMM file that is computed by the NMC and transmitted in advance to the CAD of the transmitter. Another implementation is possible using the interface 4 for addressing each receiver.

The interface 2 can be implemented on the public switched telephone network, or on the public switched packet network, or even on a diskette or a PCMCIA memory card.

I.3.5 Implementation of the interface 4

The interface 4 connects the NMC to a smart card, via a CAD. The CAD initializes it.

It is mainly used for the supervision of the smart cards connected to the CAD. The supervision of the cards consists of:

– surveying the impulse pay-per-view stored in the card;

– cleaning the EEPROM of the card. If a card has no memory left, the NMC removes the old authorizations.

Additionally, as indicated above, interface 4 may be used to send EMMs.

The interface 4 can be implemented using the public switched telephone network or the public switched packet network.

The log-in information is stored in the smart card in an ad hoc facility block. The call is initiated by the CAD upon reception of an EMM for modem wake-up.

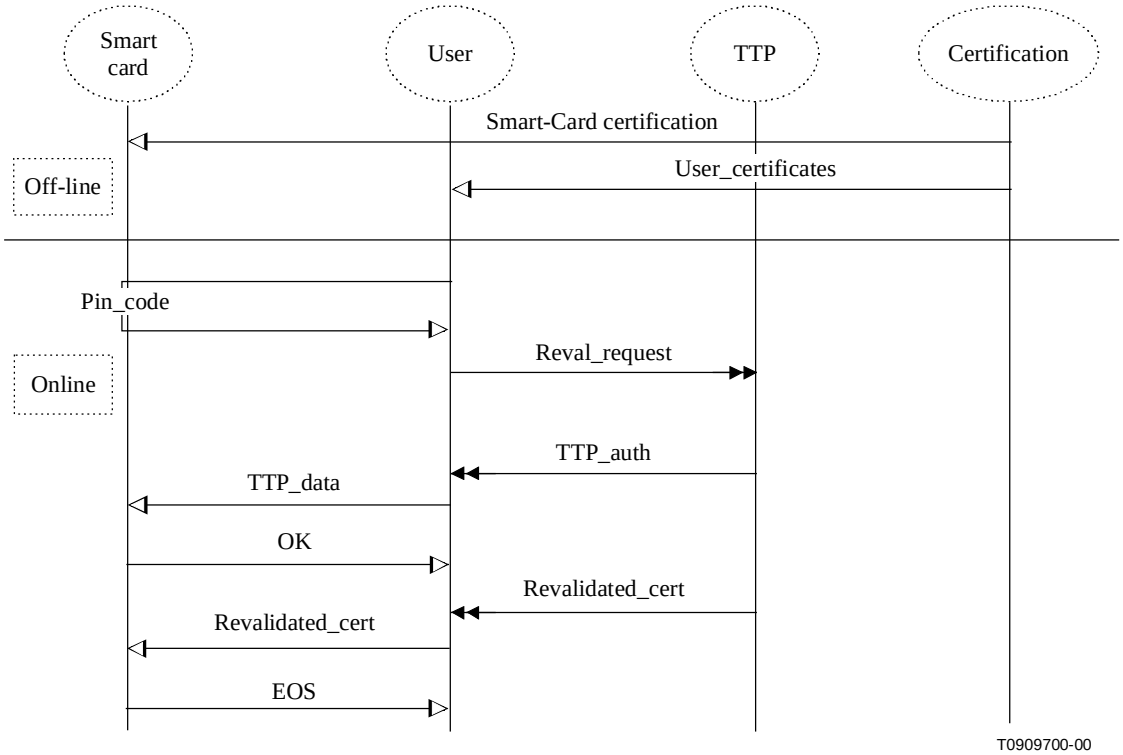
I.3.6 Main bidirectional protocols

Protocols corresponding to each mode can be presented. Here is a sequence diagram for the most important ones, considering the availability of a bidirectional low bit rate data channel between the management device and the communication sites. These protocols pave the way for a facilitated management, a large range of new services and a facilitated recovery policy.

I.3.6.1 Certificates revalidation

In order to facilitate among others the blacklisting of a user, the controller should periodically revalidate the certificates in the smart cards of the communication sites. Until the management is exclusively in charge of the NMC, this phase becomes much less relevant. The public keys database of the TTP (controller) is the same as for the management.

In Figure I.3, the TTP represents ONE role of the controller. The User is responsible for the smart card (the one who knows the pin code) on the communication site.



Double black arrows represent the messages; single white arrows represent data flows.

Figure I.3/J.96 – Certificate revalidation sequence diagram

For other services sharing the CAS security, other TTPs might be introduced. SPKI certificates servers are emerging on the Internet and can be used for electronic commerce, VPN, etc. It implies a cross-certification between TTPs and would thus be initiated with the agreement of the NMC, avoiding security compromising.

I.3.6.2 Request for entitlement

In Figure I.4 are the messages in case of bidirectional channel between the NMC and the communication sites. Notations are the same as for the previous clause.

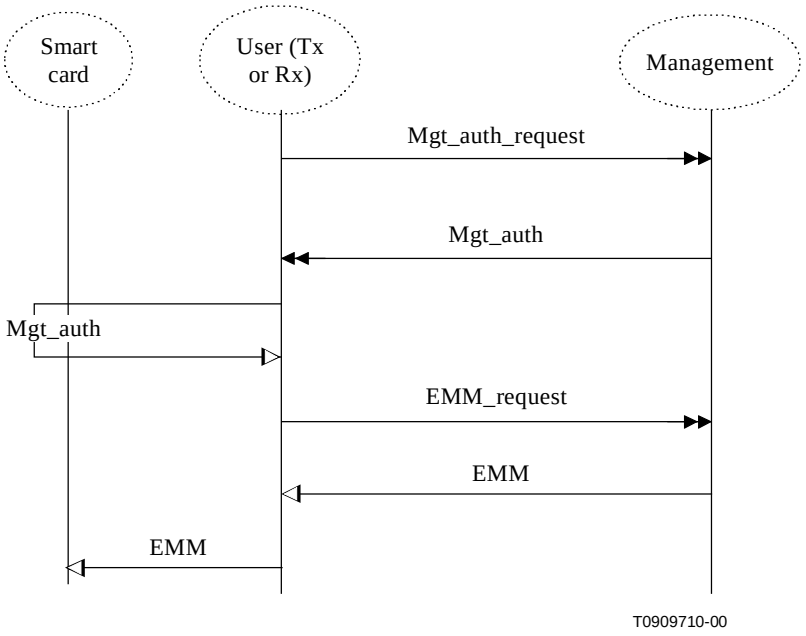


Figure I.4/J.96 – Entitlement request

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

Geneva, 2001