INTERNATIONAL TELECOMMUNICATION UNION

ITU-T J.91

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(08/94)

TELEVISION AND SOUND TRANSMISSION

TECHNICAL METHODS FOR ENSURING PRIVACY IN LONG-DISTANCE INTERNATIONAL TELEVISION TRANSMISSION

ITU-T Recommendation J.91

(Previously “CCITT Recommendation”)

FOREWORD

The ITU-T (Telecommunication Standardization Sector) is a permanent organ of the International Telecommunication Union (ITU). The 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 Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, March 1-12, 1993).

ITU-T Recommendation J.91 was prepared by ITU-T Study Group 9 (1993-1996) and was approved under the WTSC Resolution No. 1 procedure on the 22nd of August 1994.

NOTE

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

CONTENTS

SUMMARY

This Recommendation constitutes a common standard for a conditional access system for long-distance international transmission of digital television according to Recommendation J.81[1)]. It first gives an overview of any conditional access system, describing the categories of conditional access messages which need to be transmitted. It specifies a transport protocol based on HDLC frames for the conditional access messages sent in channel CA1 of Recommendation J.81.

Furthermore, an architecture of the whole transmission system, including the conditional access features, is described. This architecture differs from the traditional pay-TV systems architecture in the way that it stresses the need for an access control authority which is not co-sited with the transmitters.

The main conditional access equipments and interfaces needed to operate the conditional access system are also modelled. Their functionalities are described and some implementations are proposed, depending on the application. Lastly, practical implementations are also provided depending on the level of security and functionality required by the application.

1) Recommendation J.81 was formerly ITU-R Recommendation CMTT.723.

Recommendation J.91

TECHNICAL METHODS FOR ENSURING PRIVACY IN LONG-DISTANCE INTERNATIONAL TELEVISION TRANSMISSION

(Geneva, 1994)

The ITU-T,

considering

(a) that radio signals are by their very nature likely to be received by a large number of unidentified receivers and that in the case of international television transmission using telecommunication satellites, stations to which the information is not addressed may receive and interpret the signals;

(b) that the number of stations capable of receiving such signals is steadily increasing;

(c) that undesired access to the transmitted signal is facilitated when similar technical characteristics are used for broadcasting as those used in transmission;

(d) that Recommendation J.81 which defines the bit-rate reduction codec to be used for contribution-quality applications to the third hierarchical level of Recommendation G.702 takes into account the need for a conditional access system,

recommends

that technical methods that should be used for ensuring privacy in long-distance international television digital transmission according to Recommendation J.81 using Radiocommunication techniques should be characterized as follows.

1 Scope

This ITU-T Recommendation constitutes a common standard for a conditional access system for long distance international transmission of digital television according to Recommendation J.81.

It defines the interfaces and equipment needed to operate the conditional access system and specifies a transport protocol of conditional access messages in channel CA1 of Recommendation J.81.

Practical implementations are also provided in annexes.

2 References

- Recommendation J.81, *Transmission of component-coded digital TV signals for contribution-quality applications at the third hierarchical level of Recommendation G.702*.
- EN 50094: 1992, *Access control system for the MAC/Packet family: EUROCRYPT*.
- ISO 7816-1:1987, *Identification cards - Integrated circuit(s) cards with contacts – Part 1: Physical characteristics.*
- ISO 7816-2:1988, *Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts*.
- ISO/IEC 7816-3:1989, *Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols*.

3 Terms and definitions

For the purpose of this Recommendation, the following definitions apply:

scrambling is defined as 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).

descrambling is defined as 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

For the purpose of this Recommendation, the following abbreviations are used:

ACS	Access Control System
Bit	A contraction of the words “binary digit”
CA	Customer Address
CA1	Conditional Access channel 1 (part of the service multiplex of the codec)
CA2	Conditional Access channel 2 (part of the service multiplex of the codec)
CAD	Conditional Access Device
CD	Controller Device
CI	Command Identifier
CIW	Container Identification Word
CMSM	Control Major Security module
CW	Control Word
ECM	Entitlement Control Message
ECW	Even Control Word
EEPROM	Electrically Erasable Programmable Read Only Memory (integrated circuit)
EMM	Entitlement Management Message
HDLC	High level Data Link Control
IW	Initialization Word loaded into pseudo-random sequence generators for descrambling
LI	Length Indicator
MD	Manager Device
MH	Message Header
MMSM	Management Major Security Module
NMC	Network Management Centre
Octet	A sequence of 8 bits operated on as a data group or word
OCW	Odd Control Word
PCMCIA	Personal Computer Memory Card International Association

PPI	Phase Parity Identifier indicating which CW must be used for descrambling
PRG	Pseudo-Random (sequence) Generator
PSPN	Public Switched Packet Network
PSTN	Public Switched Telephone Network
UA	Unique Address
USM	User Security Module
SA	Shared Address
Word	A group or sequence of bits treated together

5 System overview

A conditional access system is used to enable authorized users to descramble the components of a service.

The scrambling and descrambling processes are specified in Recommendation J.81 and summarized in 5.1. These processes are performed respectively by the encoders and the decoders.

The information required for descrambling may be either manually introduced in the decoder (i.e. local control word) or provided by the conditional access system summarized in 5.2.

From the transmitter to the receiver(s), this information is structured in secure messages multiplexed with the signal itself in channels CA1 and CA2 (see clause 12/J.81). These messages are extracted from the signal by the decoders and interpreted by the conditional access system in the authorized receiver(s) in order to control the descrambling of the service components.

5.1 General description of the scrambling/descrambling processes

Figure 1 illustrates the scrambling/descrambling processes.

Conditional access requires that the television signals are scrambled by the encoder before it is transmitted. This process is under the control of a scrambling sequence obtained from a pseudo-random generator.

The descrambling process in the decoders requires the corresponding sequence (in this case the descrambling sequence) to recover the original signal.

To provide this sequence and to ensure synchronism between the transmitter and the receiver(s), the starting condition of the pseudo-random generator is controlled by an initialization word.

Conditional access to a service is in fact equivalent to conditional access to the initialization word, which results from a combination of the initialization modifier and the control word.

The initialization modifier is used in order to produce a new initialization word for each TV container, as defined in Recommendation J.81. The initialization modifier, called CIW in Recommendation J.81, is transmitted in clear in channel CA2.

Independently of the scrambling/descrambling processes, the conditional access system creates pairs of active control words. Each pair consists of an Even Control Word (ECW) valid for even blocks and an Odd Control Word (OCW) valid for odd blocks. The parity of the transmitted block is given by the indicator PPI in channel CA2 (see clause 12/J.81).

The control word is the basic element of security. Its arbitrary value remains constant during any block of TV containers (65 534 TV containers, which corresponds to 8.2 seconds). The encoder receives cryptograms of control words and transmits them to the decoder(s) through channel CA1.

5.2 General description of the conditional access system

The role of the conditional access system is to create for each new transmission a new sequence of control words and to exclusively distribute each sequence to the relevant users (one transmitter and one or more receivers, according to the configuration of the transmission). To do this, the conditional access system creates, transmits and uses conditional access messages.

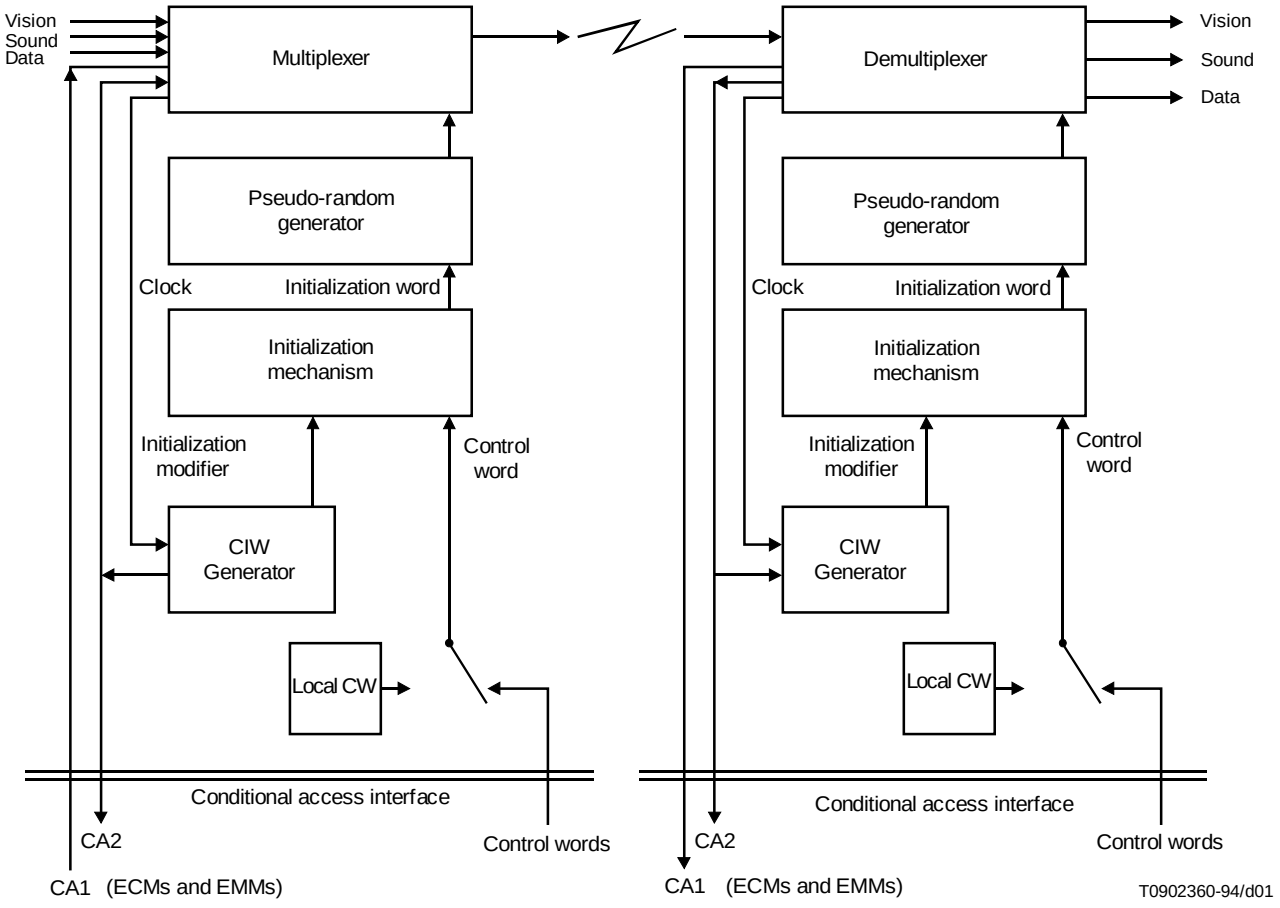

FIGURE 1/J.91

Scrambling/descrambling processes

To achieve security of the conditional access messages, two sets of cryptographic mechanisms are used:

- Block encipherment and decipherment are used for ensuring privacy (e.g. for conveying control words and keys in cryptograms).

- Cryptographic checksum computation and verification are used for ensuring integrity (e.g. for authenticating messages).

Block encipherment and cryptographic checksum computation are achieved by Major Security Modules.

Block decipherment and cryptographic checksum verification are achieved by User Security Modules.

A cryptographic checksum must protect each conditional access message where one or more cryptograms are present. Upon reception of such a message, any Security Module has to find valid the cryptographic checksum before continuing the process. Consequently, the decipherment of any cryptogram is conditioned by a successful verification of the integrity of the whole conditional access message.

In any conditional access system, an authority is needed to generate the control words and to compute and transmit their cryptograms. The authority exclusively possesses and uses the Major Security Modules.

In many traditional pay-TV systems, the same actor plays at the same time the role of the authority and the role of the transmitter. In this Recommendation, the role of the authority is deliberately separated from the role of the transmitter for the following two reasons:

– The dissemination of Major Security Modules is highly undesirable.

– The management of international television exchanges may be centralized (e.g. EBU).

Consequently, the transmitter and the receiver(s) only hold and use User Security Modules.

Two categories of conditional access messages are used by the conditional access system: the Entitlement Checking Messages (ECM) and the Entitlement Management Messages (EMM).

Channel CA1 is dedicated to the transmission of messages from the transmitter to the receiver(s). The average length of the conditional access messages is about 300 bits. An error protection (e.g. by a Golay code) may double this length. One new ECM is sent at least every 8.2 seconds. If the ECM is repeated every second, about 7 kbit/s are available to send 10 EMMs per second.

Each conditional access message is a string of optional parameters. One parameter is intended for conveying one or more cryptograms. Another parameter is intended for conveying one cryptographic checksum.

5.2.1 Entitlement Checking Messages (ECMs)

The ECMs are intended for providing with control words all the authorized users and only the authorized users. Consequently, the essential parameter of each ECM is one or more cryptograms of control word.

The ECMs may begin with one or more access criteria. If so, at least one access criterion has to be found valid by the User Security Module before continuing the process of the message.

The last parameter of each ECM must be a cryptographic checksum protecting the whole message.

5.2.2 Entitlement Management Messages (EMMs)

The EMMs are intended for providing the relevant User Security Modules with appropriate entitlements and keys. Those entitlements and keys are used to decipher cryptograms of control word transmitted in ECMs.

The main parameters of the EMMs are addresses of User Security Module, entitlements, cryptograms of key and finally, a cryptographic checksum protecting the whole message.

6 Modelling interfaces and equipment

Figure 2 gives a model of the interfaces based on the above general description.

The upper part of the figure represents the authority. The Management Device and the Control Device may not be located at the same place.

The lower part of Figure 2 represents the users, each user being in principle able to transmit and receive.

6.1 List of interfaces

– *Interface 1* – This interface ensures the transmission of EMMs from the Management Device to the Control Device. These EMMs will be used to configure the User Security Modules involved in the planned exchange of television programme.

– *Interface 2* – This interface ensures the transmission of messages (EMMs followed by ECMs) from the authority (Control Device) to the transmitter (Conditional Access Device). The transmission (at most 8 kbit/s) may be performed in real time by a dedicated channel or by a telephone line. The transmission may alternately be performed by a diskette sent by mail in advance. The messages (EMMs and ECMs) are processed by the conditional access device for insertion in channel CA1.

– *Interface 3* – This interface connects the security modules to various devices such as the Conditional Access Devices for the users and the Control and Management Devices for the authority. A possible implementation of the security module is the smart card. In this case, this interface is specified in the series of International Standard ISO/IEC 7816.

– *Interface 4* – This interface connects the Conditional Access Devices of the users to the encoders and decoders. This interface is specified in Recommendation J.81.

– *Interface 5* – This interface connects the User Security Modules of the users to the Management Device, through the Conditional Access Devices. The information consulted in the user security modules may be used for statistics and financial purposes. The interface 5 can be implemented using the public switched telephone network or the public switched packet network.

– *Interface 6* – This interface allows the dialogue with the local operator. It introduces a Man-Machine Interface on the Control and Management Devices as well as on each Conditional Access Device.

Implementations details (protocol, physical implementation) of interfaces 1, 2, 5 and 6 are application dependent and are not provided by this Recommendation.

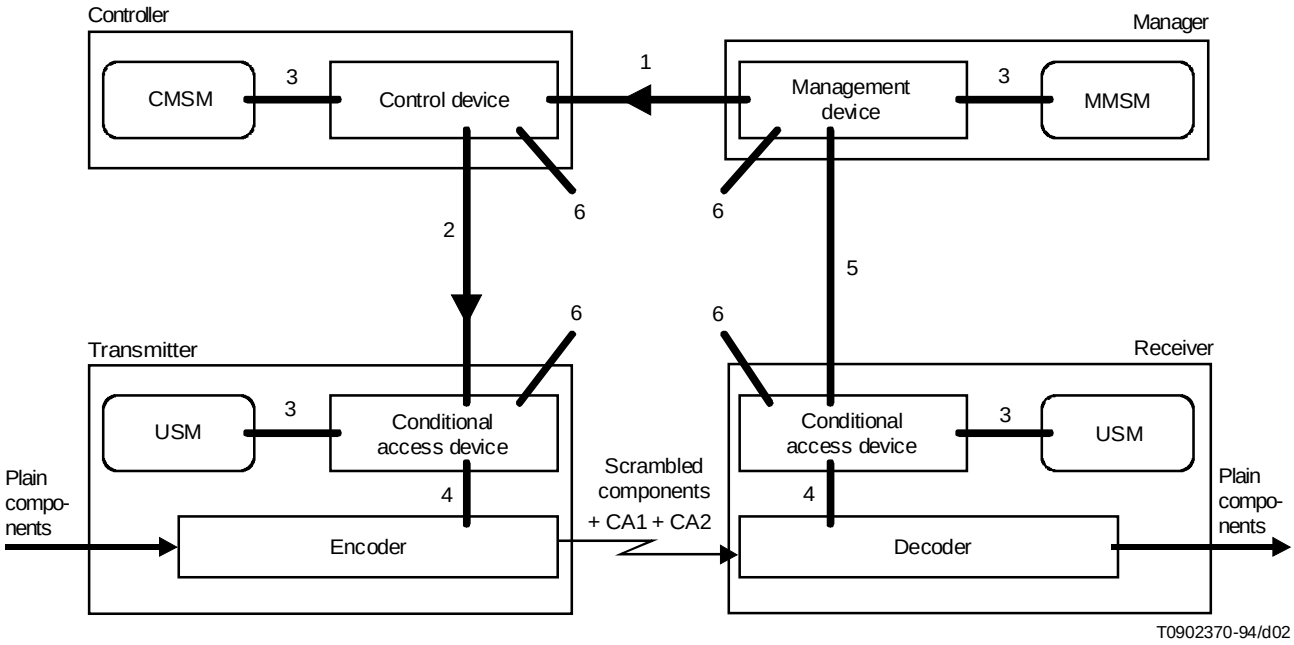

FIGURE 2/J.91

Interface modelling

6.2 List of equipment

Encoders and decoders are described in Recommendation J.81.

The Control and Management Major Security Modules (capable of performing block encipherment and cryptographic checksum computation) are used to compute respectively the ECMs and the EMMs.

The User Security Module (capable of performing block decipherment and cryptographic checksum verification only) is used to interpret the ECMs and EMMs. It stores the entitlements and the keys of its user to decipher the cryptograms of the control words. It may also store the actual accesses of the user to the system in case of impulse pay-per-view.

Any Security Module may be implemented as a smart card. In this case, the Major Security Modules are sometimes called “mother cards” and the User Security Modules “daughter cards”.

The Management Device is connected to one or more Management Major Security Modules which compute the EMMs. Those EMMs are sent via the Control Device to the user. If the number of users is a few thousands, the Management Device can be implemented as a personal computer.

The Control Device randomly generates the control words and constructs the ECMs with the help of its Control Major Security Modules. Those ECMs, as well as the EMMs communicated by the Management Device, are sent to the transmitter. If the number of users is a few thousands, the Control Device can be implemented as a personal computer.

The Conditional Access Device is connected to one or more encoders or decoders and to one or more User Security Modules. At the encoder side, this device generates channel CA1 which conveys EMMs and ECMs to the receiver(s). The Conditional Access Device receives EMMs and selects the EMMs addressed to its Security Module(s). It also receives ECMs which are processed by the User Security Modules.

The "access control system" (ACS) described in Recommendation J.81 corresponds to the combination of a Conditional Access Device with one or more User Security Modules.

7 Transport protocol of conditional access messages in channel CA1

The conditional access messages are broadcast in channel CA1 at the nominal bit rate of 8 kbit/s (see Recommendation J.81).

Two types of conditional access messages have been described so far: the ECMs and the EMMs.

Depending on the encryption mode (see 12.7.3/J.81), there may be:

- no ECM at all (modes 0 and 1);
- one new ECM every block (mode 2);
- several new ECMs every block (mode 3).

In mode 3, each ECM shall be associated with the components to which it applies.

The EMMs can be sent to:

- *All users* – In this case, they are called EMM-G and sent without address.
- *A group of users* – In this case, they are called EMM-S and sent with a shared address (SA, 24 bits).
- *A unique user* – In this case, they are called EMM-U and sent with a unique address (UA, 36 bits).

ECMs and EMMs are secured with cryptographic algorithms. The reference of the crypto-algorithm which is used, has to be sent together with the message.

The same ECMs and EMMs have to be sent several times [e.g. the ECM is changed every block (8.2 seconds) but the same ECM can be repeated every second to reduce the acquisition delay]. A mechanism has to be provided to allow the receivers to distinguish new conditional access messages from repeated ones.

7.1 Transmission frame

The frame structure described in 9.2.4/J.81 is used for the transmission of the conditional access messages. It is based on an HDLC (High level Data Link Control) frame structure.

The transmission frame is composed of the following information, illustrated in Figure 3:

- a beginning flag (START): "01111110";
- a Message Header (MH): 2 octets;
- a conditional access message: n octets;
- a 16-bit error-detecting CRC (FCS: Frame Check Sequence) (CRC): 2 octets;
- an ending flag, identical to the beginning one (END): 1 octet.

To avoid the imitation of flags by data, HDLC defines a method of suppressing long strings of ones in the data and CRC areas.

For each transmitted octet, bit 0 is the least significant bit and is sent first according to HDLC specification. However, octets are sent, the most significant octet first.

After the end flag, the HDLC line returns to the "idle" mode.

FIGURE 3/J.91

Frame structure

The 2 MH octets are coded as described in Tables 1 and 2.

Messages which are not recognized by the receiver should be ignored.

In encryption mode 3 (see 12.7.3/J.81), several ECMs preceded by their associated Message Header can be sent in one single HDLC frame.

TABLE 1/J.91

Coding the Message Header for conditional access messages

b_{16}	b_{15}	b_{14}	b_{13}	b_{12} Bit$_7$	b_6 b_1	Meaning
0	0	0	0	RFU	See Table 2	ECM
0	0	Other value		RFU	See Table 2	Reserved for up to 3 special types of ECM
0	1	0	0	RFU	1 1 1 1 1 1	EMM-U
0	1	0	1	RFU	1 1 1 1 1 1	EMM-S
0	1	1	0	RFU	1 1 1 1 1 1	EMM-G
Any other value				RFU	1 1 1 1 1 1	Reserved for up to 9 other types of EMM
NOTE – The bits b_{12} to b_7 are reserved for future use (RFU) and set to 0.						

TABLE 2/J.91

Meaning of the bits b_6 to b_1 of the Message Header for ECMs

b_6	b_5	b_4	b_3	b_2	b_1	Meaning
0	0	0	0	0	0	RFU
0	X	X	X	X	1	The component T is concerned by the ECM
0	X	X	X	1	X	The component A is concerned by the ECM
0	X	X	1	X	X	The component T′ is concerned by the ECM
0	X	1	X	X	X	The component A′ is concerned by the ECM
0	1	X	X	X	X	The component V is concerned by the ECM
Any other value						RFU

7.2 Conditional access message content

7.2.1 Command Identifier (CI)

All ECMs and EMMs contain an 8-bit Command Identifier field (CI) that describes the format being used for the message field and the type of cryptographic algorithm used. Its coding is described in Figure 4.

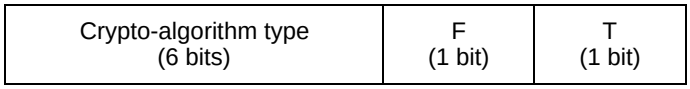

FIGURE 4/J.91

Command Identifier (CI) coding

NOTES

1 Type of crypto-algorithm (6 bits) – This parameter is used to identify simultaneously up to 64 types of crypto-algorithm. Only those messages having a type matching with the type of the user security module can be interpreted and processed by the user security module of the receiver.

2 F is a bit describing the format of the data field of the message.

a) F = 1 – The data field is structured in the variable format defined by EUROCRYPT.

b) F = 0 – Reserved for future use.

3 T is the toggle bit. It is maintained in the same state as long as the content of the message has not changed. It is used in EMMs-G and in ECMs to indicate a change in the information content of those messages. It has no meaning for the EMMs-U and EMMs-S.

7.2.2 ECM content

The ECM is described in Figure 5, before insertion in a frame.

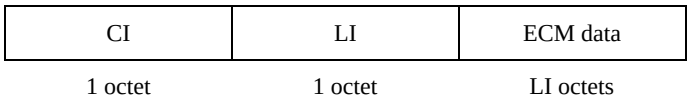

FIGURE 5/J.91

ECM message

7.2.3 EMM content

The EMM is described in Figure 6, before insertion in a frame.

FIGURE 6/J.91

EMM message

All EMMs, except EMM-G start with a Customer Address (CA). The length of the CA field is:

- 40 bits for EMM-U – In this case, the first 4 bits are set to 0 and the last 36 bits transport the UA (Unique Address).
- 24 bits for EMM-S – In this case, CA transports the 24 bits of the Shared Address (SA).

8 Practical implementations

In practice, the functionalities described above can be implemented in various ways, ranging from the setting of local control words only through proprietary conditional access systems for small or simply-configured networks to large fully-featured, commercially available conditional access systems that might be used in an open network environment, or where the number of subscribers to the network, and the variety of access control functions needed is large.

Operation with a local control word is described in Annex A. Operation with the EUROCRYPT[2)] conditional access system, which covers all the functions discussed in the subclause above, is described in Annex B while other systems that might be added will be included in subsequent annexes.

Annex A

Operation with local control word

(This annex forms an integral part of this Recommendation)

A.1 Practical implementation with a local control word

Local control words may be used. This means that the encoder at the Communication Site for transmission uses only one control word during a whole transmission. Such a control word has to be entered into the encoder by the operator of the transmitter. In order to descramble the signal at the Communication Site for reception, the decoder has to get the same control word from the operator of the receiver.

Such an implementation implies a new specific action of the operator. Although this implementation is a lot less secure from the access control point of view, it would actually be totally independent of the Management and Control Devices and of the CAD, and could coexist easily with an access control system.

Annex B

Operation with EUROCRYPT[3)]

(This annex forms an integral part of this Recommendation)

B.1 Introduction

This annex describes a practical implementation using the fully-featured standardized EUROCRYPT conditional access system where the functionalities of the various security modules are provided by the family of PC2 smart cards.

EUROCRYPT is a conditional access system standardized by UTE (EN 50094, 1992) and currently used for controlling access to D2MAC/Packet signals. It specifies the ECMs and the EMMs.

The PC2 family of smart cards consist of security modules that have been developed to implement the security functions of EUROCRYPT. There are several categories of PC2 smart cards (see Figure B.2):

- the PC2 management mother cards provide the functions of the Management Major Security Modules;
- the PC2 control mother cards provide the functions of the Control Major Security Modules;
- the PC2 daughter cards provide the functions of the User Security Modules.

---

2) EUROCRYPT is standardized by UTE (EN 50094, 1992).

3) EUROCRYPT is standardized by UTE (EN 50094, 1992).

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, synchronization between transmitters and receivers.

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.

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.

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

Figure B.1 illustrates the network considered from the access control point of view. In Figure B.1 and in the subsequent clauses, the Network Management Centre is currently abbreviated as NMC and the Conditional Access Devices as CADs.

PC2 mother cards are only necessary in the Network Management Centre.

One or more PC2 daughter cards are used for transmitting and for receiving at each Communication Site.

B.1.1 Programmes and transmissions

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.

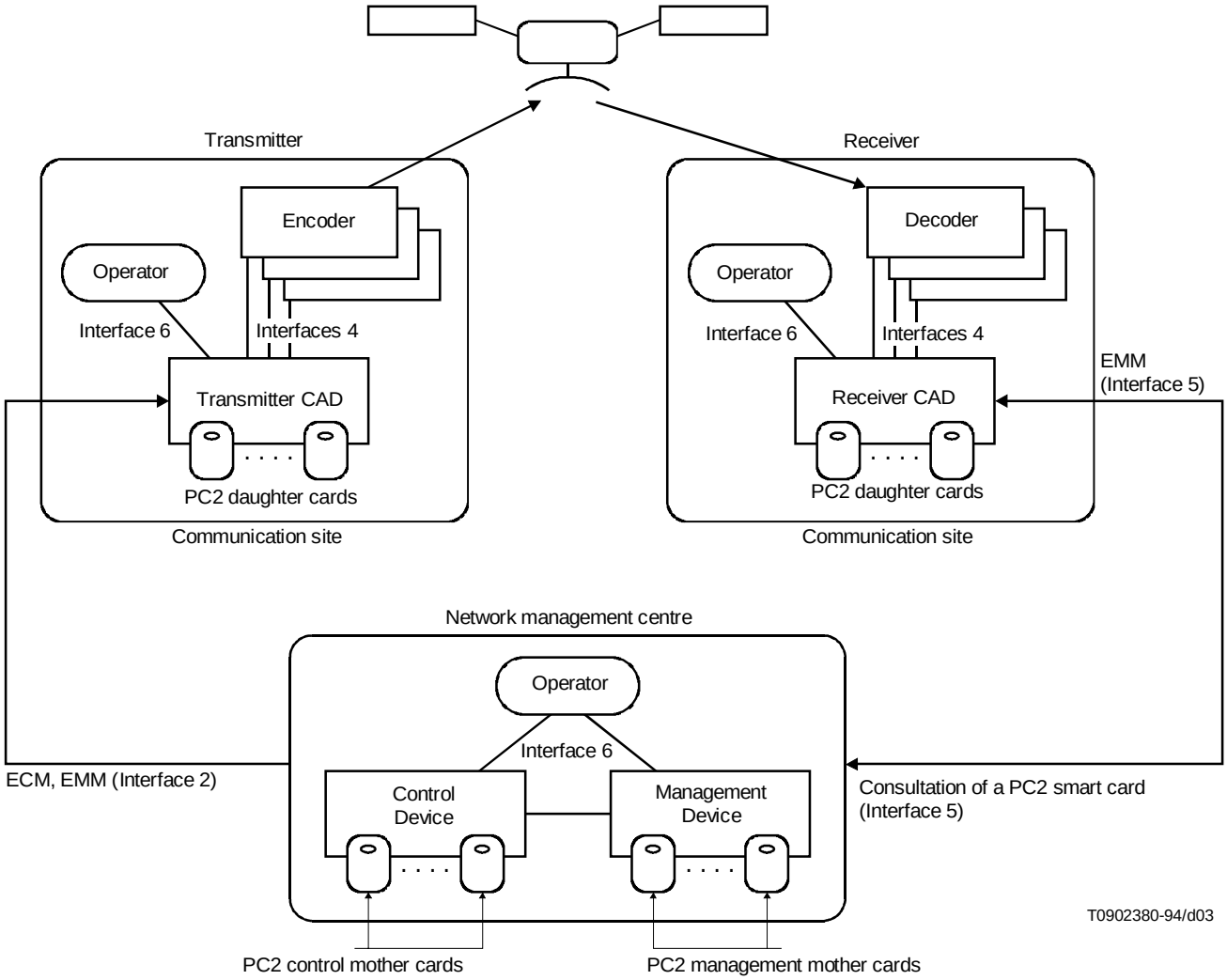

FIGURE B.1/J.91

Architecture of the network

B.2 Functionalities of the Network Management Centre (NMC)

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 controls the issue of all the smart cards of the system and ensures the supervision of all the daughter cards.

Figure B.2 gives a schematic of a NMC.

B.2.1 ECM generation

The NMC has to generate the ECMs. For that, the NMC generates control words, enciphers those control words using a mother card and creates the corresponding ECMs. Each ECM is protected by a cryptographic checksum computed by this mother card. During the transmission, a new ECM is used every 8.2 seconds. The ECMs are sent to the CAD of the transmitter through the interface 2.

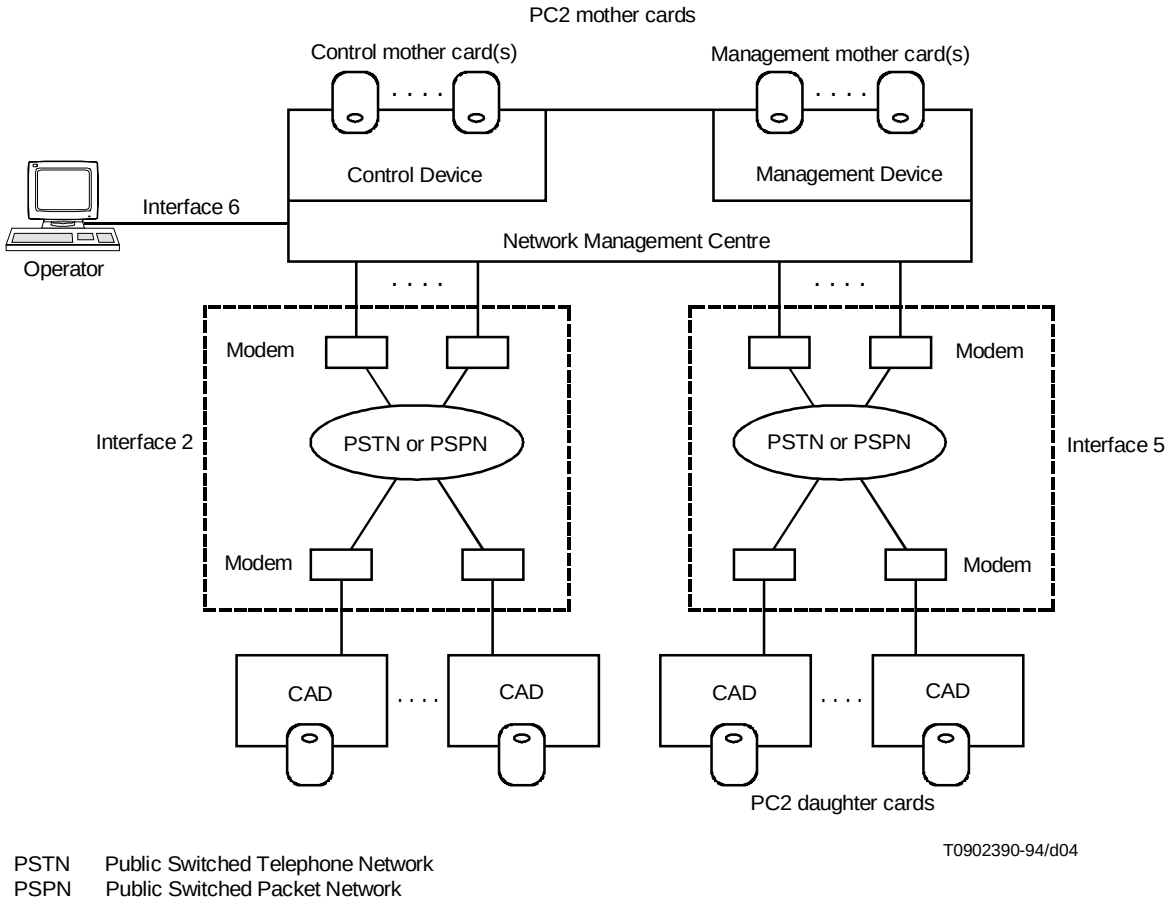

FIGURE B.2/J.91

Network Management Centre (NMC)

One immediate way of implementing the scheme is to regularly create ECMs and to send them "on-line" 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 over-run, 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. Using EUROCRYPT ECMs, a file of 16 k octets provides ECMs for about one hour of programme.

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.

B.2.2 EMM generation

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

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

The other EMMs are for the receivers. They will allow authorized daughter 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 5 (via phone, X.25, 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.

Two categories of EMMs are defined: EMMs-U and EMMs-S.

An EMM-U contains the unique address of only one daughter card. Consequently to distribute a given entitlement to *n* daughter cards would imply the computation and the transmission of *n* EMM-U.

An EMM-S contains the shared address of a group of daughter cards. One EMM-S can address up to 256 daughter cards sharing the same management key. Using EMM-S reduces the average number of EMMs that should be built and transmitted for a TV transmission.

B.2.3 Supervision of daughter cards

The NMC manages the contents of each daughter card.

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

The NMC has a database to know the contents of all smart cards and detailed information about all CADs (locations, smart cards, etc.).

If a daughter card has no memory left, the NMC has to clean the memory by removing the obsolete keys and the obsolete entitlements. If the cleaning is not possible (PC2-1 card), the NMC advises its operator and the CAD operator to change the daughter card.

B.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.

B.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).

B.3 Implementation of the CADs

The behaviour of the CAD of the transmitter consists of:

- transmitting the relevant EMM(s) to its daughter card(s) in order to store new key(s) and entitlement(s);
- regularly (every 8.2 seconds) transmitting one ECM to its daughter card to get back the corresponding CW that should be given to the encoder to scramble the TV programme;
- regularly (every 1 second) transmitting to the encoder one ECM to broadcast to the decoders (via the CA1 channel in the 34 Mbit/s multiplex);
- if needed, transmitting also the EMMs to the encoder to send to the decoders (via the CA1 channel in the 34 Mbit/s multiplex).

The behaviour of the CAD of the receiver consists of:

- getting the relevant EMMs from the decoder or from the direct link with the NMC and transmitting it to its daughter card(s) in order to store new key(s) and entitlement(s);
- regularly getting the ECMs from the decoder and sending them to its daughter card to get back the corresponding control words, and to give back to the decoder these control words.

Figure B.3 illustrates the architecture of the CAD.

The ECMs and EMMs transmitted in the channel CA1 may be protected by a Golay code. In this case, before transmission, the transmitter has to protect these messages by a Golay code and on reception, each receiver has to correct the messages before further processing.

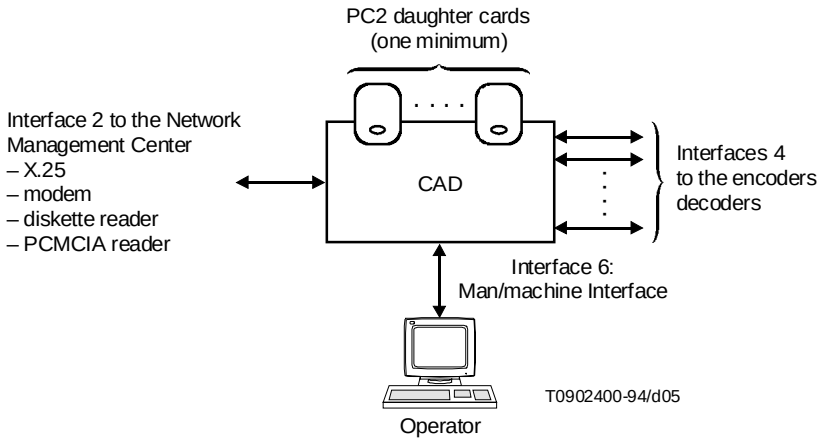

FIGURE B.3/J.91

Architecture of the CAD

B.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 or a PCMCIA memory card) 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.

This mode is very appropriate when using impulse pay-per-view. The daughter 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.

B.4 Implementation of the interface 2

The interface 2 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 "on-line" 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 5 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.

B.5 Implementation of the interface 5

The interface 5 connects the NMC to a daughter card, via a CAD. It is initialized by the CAD.

It is mainly used for the supervision of the daughter 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 (PC2-2 cards only). If a card has no memory left, the NMC removes the old authorizations. If the cleaning is not possible (PC2-1 card), the NMC advises its operator and the CAD operator to change the daughter card.

Additionally, as indicated above, interface 5 may be used to send EMMs.

The interface 5 can be implemented using the public switched telephone network or the public switched packet network.

The log-in information is stored in the daughter card in an ad-hoc facility block. The call is initiated by the CAD upon reception of an EMM for modem wake up (see EUROCRYPT Specifications, Appendix 2, § 11).

B.6 Illustration of the system using EUROCRYPT features

To compute the control words from a cyclic file of ECMs associated to a given transmission, the PC2 daughter card of the receiver must contain the correct authorization key and at least one valid entitlement. The keys and the entitlements are defined by the NMCr which sends EMMs to authorize the relevant cards. To perform this action, the NMC has the choice between several operational modes described below.

The abbreviations used in this clause for representing the content of the ECMs and EMMs are defined by EUROCRYPT (EN 50094, 1992), with further details on the use of EMM-U and EMM-S.

B.6.1 Access control facility by updating the authorization key

The authorization keys of all relevant cards may be updated before each new programme. The following EMM-U is intended for updating an authorization key in the card addressed by UA:

EMM-U (37 octets): UA, CI LI, PI LI PPID, PI LI IDUP, PI LI Enciphered Key, PI LI HASH

B.6.2 Access control facility by subscription

The NMC can send subscriptions to selected cards. A subscribed card has access to a category of programmes during a given period of time. The following EMM-U is intended for appending a subscription in the card addressed by UA:

EMM-U (30 octets): UA, CI LI, PI LI PPID, PI LI DATES+TH/LE, PI LI HASH

B.6.3 Access control facility by a programme number

The NMC can associate a number to each programme (PNUMB). The following EMM-U is intended for appending an entitlement booking one or more consecutive programme numbers in the card addressed by UA:

EMM-U (30 octets): UA, CI LI, PI LI PPID, PI LI INUMB+FNUMB, PI LI HASH

An alternate solution consists of using one or more EMMs-S preceded by one EMM-G. A group of up to 256 cards is addressed by SA. Each card in the group has a rank, valued from 1 to 256. A given card in the group accepts or rejects the action depending on whether the ith bit of ADF is valued to 1 or 0:

EMM-G (15 octets): CI LI, PI LI PPID, PI LI INUMB+FNUMB

EMM-S (79 octets): SA, CI LI, ADF, PI LI HASH

With only one EMM-G + EMM-S, it is possible to send an entitlement selectively in a group of 256 cards. This mode is very attractive for programmes which are planned a long time before their transmission.

B.6.4 Access control facility by impulse pay-per-view to a programme number

In this mode, no EMMs are required for the receivers. All potential receivers having the correct authorization key can descramble the programme in pay-per-view mode (with the agreement of the receiver operator). The card memorizes the action of the operator. This mode is very attractive for urgent transmission.

B.6.5 ECMs with the last three access criteria

Several access modes can be used together for the same programme. In such a case, several classes of receivers are accessing to the same programme:

- subscribers have an access by subscription;
- booked users have an access by programme number;
- late users may have an access by impulse pay-per-view access to a programme number.

The following ECM proposes the access by subscription, by booking and by impulse pay-per-view. The card checks the access criteria in the order until finding a valid entitlement:

ECM (53 octets): CI LI, PI LI PPID, PI LI DATE+TH/LE, PI LI PNUMB, PI LI PNUMB+PPV-P, PI LI ECW/OCW, PI LI HASH

Annex C

Operation with other systems

This annex is for further study.