



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.91

(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.

© ITU 1995

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

	Page
1 Scope	1
2 References	1
3 Terms and definitions	2
4 Abbreviations	2
5 System overview	3
5.1 General description of the scrambling/descrambling processes	3
5.2 General description of the conditional access system	3
6 Modelling interfaces and equipment	5
6.1 List of interfaces	5
6.2 List of equipment	6
7 Transport protocol of conditional access messages in channel CA1	7
7.1 Transmission frame	7
7.2 Conditional access message content	9
8 Practical implementations	10
Annex A – Operation with local control word	10
A.1 Practical implementation with a local control word	10
Annex B – Operation with EUROCRYPT	10
B.1 Introduction	10
B.2 Functionalities of the Network Management Centre (NMC)	12
B.3 Implementation of the CADs	14
B.4 Implementation of the interface 2	15
B.5 Implementation of the interface 5	16
B.6 Illustration of the system using EUROCRYPT features	16
Annex C – Operation with other systems	17

SUMMARY

This Recommendation constitutes a common standard for a conditional access system for long-distance international transmission of digital television according to Recommendation J.81¹⁾. 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.*



Documents

Document Sharing Hub

Recommendation J.91 (08/94)

1

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.