



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.233

(11/2002)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS
Infrastructure of audiovisual services – Systems aspects

Confidentiality system for audiovisual services

ITU-T Recommendation H.233

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
SYSTEMS AND TERMINAL EQUIPMENT FOR AUDIOVISUAL SERVICES	H.300–H.399
SUPPLEMENTARY SERVICES FOR MULTIMEDIA	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569

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

ITU-T Recommendation H.233

Confidentiality system for audiovisual services

Summary

This Recommendation describes the confidentiality part of a privacy system suitable for use in narrow-band audiovisual services conforming to ITU-T Recs H.320, H.221, H.230 and H.242. Although an encryption algorithm is required for such a privacy system, the specifications of such algorithms are not all included here: the system caters for more than one specific algorithm. Some of those algorithms and their parameters are defined in Annex A. A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem as described in ITU-T Rec. H.234.

This revised version of ITU-T Rec. H.233 introduces a number of corrections and clarifications to the original version and, more importantly, introduces the description on the usage of Triple DES and AES encryption in applicable H.320.x-series Recommendations.

Source

ITU-T Recommendation H.233 was revised by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 November 2002.

FOREWORD

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

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

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

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

NOTE

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had 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.

© ITU 2003

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	Normative references.....	1
3	Abbreviations.....	1
4	Properties of the system specified	2
4.1	Confidentiality	2
4.2	Algorithm specification	2
5	The confidentiality mechanism	2
5.1	Description of operation	2
5.1.1	Controls and indication within the H.221 frame	3
5.1.2	Message formats	3
5.1.3	Unenciphered ECS channel	4
5.2	Transmission encryption method	8
5.3	Procedure for use of the system.....	9
6	Encryption of MLP channel.....	9
Annex A	– Encryption algorithms and their parameters.....	9
A.1	Scope	9
A.2	Normative References	9
A.3	FEAL	10
A.4	DES.....	12
A.5	IDEA.....	12
A.6	TDEA	12
A.7	AES.....	13
Appendix I	– Encryption and decryption for $2 \times B$ channels	15
Appendix II	– Audiovisual privacy communication procedure.....	17

.....

... ..

ITU-T Recommendation H.233

Confidentiality system for audiovisual services

1 Scope

A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem.

This Recommendation describes the confidentiality part of a privacy system suitable for use in narrow-band audiovisual services conforming to ITU-T Recs H.221, H.230 and H.242. Although an encryption algorithm is required for such a privacy system, the specification of such an algorithm is not included here: the system caters for more than one specific algorithm.

The confidentiality system is applicable to point-to-point links between terminals or between a terminal and a Multipoint Control Unit (MCU); it may be extended to multipoint working in which there is no decryption at the MCU, but this is for further study.

2 Normative references

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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [1] ITU Recommendation H.221 (1999), *Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices*.
- [2] ITU Recommendation H.242 (1999), *System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s*.
- [3] ITU Recommendation H.230 (1999), *Frame-synchronous control and indication signals for audiovisual systems*.
- [4] ITU Recommendation X.680 (2002), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- [5] ITU Recommendation H.234 (2002), *Encryption key management and authentication system for audiovisual services*.
- [6] ISO 8732:1988, *Banking – Key management (wholesale)*.

3 Abbreviations

This Recommendation uses the following abbreviations:

AIA	Audio Indicate Active (Control & indication codes) (see [3])
AIM	Audio Indicate Muted (Control & indication codes) (see [3])
BAS	Bit-rate Allocation Signal (see [1])
CRC4	4-bit Cyclic Redundancy Check (see [1])
ECS	Encryption Control Signal (see [1])

FAS	Frame Alignment Signal (see [1])
H.221	H.221 framing/frame structure (see [1])
ILC	Identifier, Length, Content
IV	Initialization Vector
LSB	Least Significant Bit
MCU	Multipoint Control Unit
MLP	MLP logical channel (see [1])
MSB	Most Significant Bit
OFB	Output feedback
SE	Session Exchange
SV	Starting Variable
TOFB	TDEA Output Feedback
VIS	Video Indicate Suppressed (Control and indication codes) (see [3])

4 Properties of the system specified

4.1 Confidentiality

- 1) Confidentiality is independent of other privacy services provided by the system; keys are provided by other mechanisms such as that described in ITU-T Rec. H.234 on Authentication and Key Management, or may be manually entered.
- 2) It is applicable to audiovisual signals framed according to ITU-T Rec. H.221, at transfer rates of $p \times 64$ kbit/s where p takes any one value from 1 to 30. In accordance with ITU-T Rec. H.221, the FAS, BAS, and ECS channels of the frame structure are not encrypted.
- 3) Confidentiality is given to all user audio, video and data transmissions, these signals being encrypted together under the same key (this currently includes MLP data, according to Annex A/H.221, though this aspect is for further study).
- 4) The system is independent of the encryption algorithm used; some algorithms are currently provided for, and further algorithms could be added.
- 5) The confidentiality mechanism is capable of working in point-to-point calls, and also in multipoint calls where decryption is permitted at the MCU (the so-called "trusted MCU").

4.2 Algorithm specification

The specification of algorithms is not included in this Recommendation, which caters to a wide range of encryption algorithms. The specifications may be defined in Annex A, or shall be available elsewhere (see 5.2) and shall contain the following details:

- lengths of initialization vector and session keys;
- generation of starting variable from initialization vector.

5 The confidentiality mechanism

5.1 Description of operation

Figure 1 gives a block diagram of a link encryptor. It consists of an encryptor block and a decryptor block. The encryptor takes in user data and enciphers it to form enciphered data. The decryptor takes enciphered data and deciphers it to obtain user data.

Two channels are needed to connect the encryptor and decryptor. One is used to transmit the enciphered user data. The second is an unenciphered channel known as the Encryption Control Signal (ECS) which is used to pass control information from the encryptor to the decryptor. Although these two channels are shown physically separated, in practice, they are multiplexed into a single frame structure as shown in ITU-T Rec. H.221.

Additive-stream encipherment techniques are used (see 5.2).

Keys are provided by other mechanisms and are presented to the confidentiality mechanism as required. They are used by the encryptor and decryptor synchronously with the data, the key-loading synchronization flag being sent via the control channel (see L in 5.1.3).

Data encipherment is controlled from the encryptor: the encryption ON/OFF flag is sent via the control channel to indicate when data is being enciphered. The decryptor responds to this flag and deciphers data when requested.

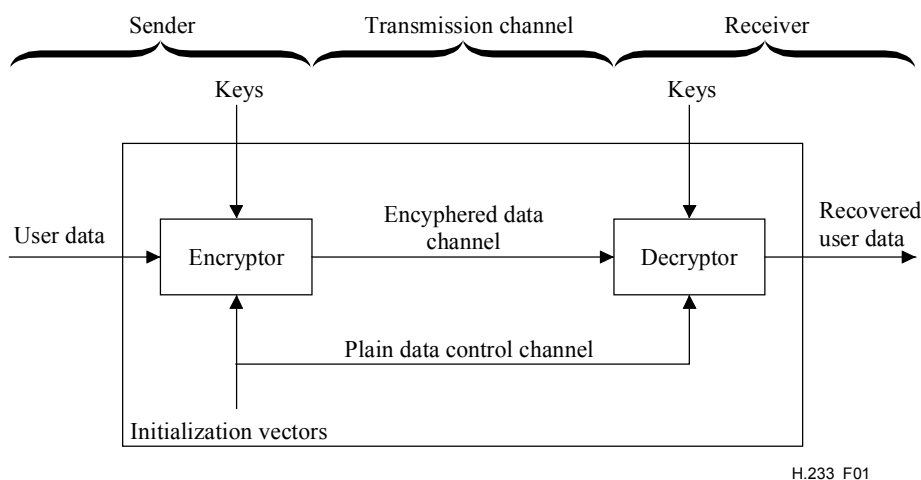


Figure 1/H.233 – Block diagram of a link encryptor

5.1.1 Controls and indication within the H.221 frame

To indicate the presence of a confidentiality system within a terminal the BAS code "Encryption capability" shall be transmitted. If this capability is signalled from both ends of a link, the Encryption Control Signal (ECS) channel may be opened in each direction by use of the encrypt-on BAS command; the ECS channel may be closed using the command encrypt-off, but this shall be preceded by the transmission of the encryption-off flag within the channel itself (see below). If a terminal receives the BAS command encrypt-off without first receiving the encryption-off flag, the user shall be alerted to a possible intrusion or malfunction of the confidentiality system.

In cases where an H.221-framed signal is in use in one direction only, the ECS channel may be activated without use of the capability mechanism: the mechanism to ensure that the receiving end is able to decrypt the chosen algorithm, etc., is outside the scope of this Recommendation.

5.1.2 Message formats

The messages used by the encryption system for key distribution and authentication are formatted in a nested ILC (Identifier, Length, Content) form as described in ITU-T Rec. X.680 [4]. The length may be encoded in short form or long form. The indefinite form as defined in [4] will not be used.

A short description of some of the ITU-T Rec. X.680 [4] definitions used within this Recommendation is given below.