



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.234

(11/2002)

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

Encryption key management and authentication system for audiovisual services

ITU-T Recommendation H.234

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.234

Encryption key management and authentication system for audiovisual services

Summary

This Recommendation describes three methods of encryption key management, namely:

- ISO 8732;
- Diffie-Hellman; and
- RSA.

They are applicable to the encryption of audiovisual signals transmitted digitally using the H.221 frame structure. The management messages defined here are transmitted within the H.221 Encryption Control Signal (ECS) channel, whose structure and use are defined in ITU-T Rec. H.233.

This revision of the Recommendation improves the overall readability of the text, removes ambiguities of certain aspects related to the exchange of asymmetric length of keys, and removes references to MLP encryption according to T.120-series Recommendations, since this effort is for further study. References to ASN.1 were also updated to the newest version of its specification.

Source

ITU-T Recommendation H.234 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.....	2
3	Message system and key exchange.....	3
3.1	Message channel.....	3
3.2	Message formats	3
3.2.1	Identifier	3
3.2.2	Length.....	4
3.2.3	Bit string	4
3.3	Starting the privacy system	4
3.3.1	Starting messages	4
3.3.2	Session key exchange.....	5
4	ISO 8732 key management.....	7
4.1	Introduction	7
4.2	Key management architecture	7
4.3	Key management environments	7
4.4	Cryptographic service message exchanges	8
4.5	Example of ISO 8732 message exchange	8
5	Extended Diffie-Hellman key distribution	9
5.1	Introduction	9
5.2	The basic protocol	9
5.2.1	*Key* exchange method	10
5.2.2	Derivation of the *key*	11
5.3	Diffie-Hellman messages	11
5.3.1	*Key* exchange information	11
5.3.2	Intermediate *key* exchange information	12
5.3.3	Check code information from MCU.....	12
5.4	Extension for line checks.....	12
6	RSA based operation	13
6.1	Introduction	13
6.1.1	General	13
6.1.2	Notation	13
6.2	System set-up.....	14
6.3	Authentication key generation and distribution	14
6.4	Certification.....	15
6.5	Alternative solution for certification without a GCA.....	16
6.6	Authentication of entities	16



Documents

Document Sharing Hub

ITU-T Rec. H.234 (11/2002)

iii

	Page
6.6.1 Simultaneous transmission of RSA.P1 messages.....	18
6.7 Generation of key for encryption of session keys	18
6.8 RSA messages	18
6.8.1 Authentication initiation.....	19
6.8.2 Authentication response	20
6.8.3 Authentication complete.....	20
6.8.4 Authentication failed	21
7 MCU operation	21
Bibliography.....	21

ITU-T Recommendation H.234

Encryption key management and authentication 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 authentication and key management methods for a privacy system suitable for use in narrow-band audiovisual services conforming to ITU-T Recs H.221, H.230 and H.242. The confidentiality specification is independent, and is contained in the separate ITU-T Rec. H.233.

Privacy is achieved by the use of *secret keys*. The keys are loaded into the confidentiality part of the privacy system and control the way in which the transmitted data is encrypted and decrypted. If a third party gains access to the keys being used, then the privacy system is no longer secure.

The maintenance of keys by users is thus an important part of any privacy system. Three alternative practical methods of key management are specified in this Recommendation. For cases where automated key management is not feasible, an unspecified alternative such as manual key management can be used.

The first is identified as ISO 8732. It is based on manually installed keys in systems that physically afford those keys a high measure of protection, and then an automated exchange of keys encrypted under the manually distributed keys. The algorithm used for encrypting these automatically distributed keys is normally the same as that used for encrypting the communication itself. The security of automatically distributed keys depends on the security of the manually distributed keys.

Automatically distributed keys may be used for a single session, or may be used for multiple sessions in a given period of time (e.g. a month). ISO 8732 contains protocols not only for the automated exchange of information between the two terminals, but also physical protocols for ensuring the security of the manual distribution of keys as well.

There are two distinct environments: direct point-to-point (two layer), where the two terminals share a common key, and a three-layer environment, where the two terminals who wish to communicate do not share a common key, but use the facilities of a mutual third party, with whom each of them do share a common key. The interfaces to the third party are outside the scope of this Recommendation, although it is required to distinguish between the two environments.

Note that session key exchange specified in 3.3.2 is functionally duplicated in X9.17, in that the keys automatically distributed in X9.17 are strong enough to be used as session keys. However, to follow the form of this Recommendation, these keys will be used as **key**, the **key** in 3.3.2.

The second is a simple yet secure method known as "extended Diffie-Hellman", which generates and exchanges keys automatically via the system itself (this key exchange is itself encrypted). It requires no action from users until keys have been exchanged; they are then advised to confirm *verbally* that the same check sequence is available at each terminal. The method is quite adequate to prevent outsiders listening in on an audiovisual call carried over a satellite channel for example. To defeat the system, it would be necessary for the interloper to intercept totally the bidirectional communication before encryption had been activated, and to exchange keys with both parties, pretending to each that it is the other legitimate party. The method does not provide authentication.

The third method is again more complex and provides a higher degree of privacy and also provides *authentication* of audiovisual service entities (terminals, MCUs, etc.). The "RSA Method" is very similar to the public key method specified in ITU-T Rec. X.509 and uses the RSA algorithm. The method requires the establishment of a security agency, available to the whole population of entities

~~~~~

which require interconnectability: certification is effectively "off-line", and relies on the integrity of the agency. This authentication mechanism allows the parties involved in a conference call to be identified to others in an assured manner, and can be operated in multipoint as well as point-to-point calls.

All methods require the use of an associated error-free clear channel. Note that Access Control, Integrity and Non-repudiation are not provided by any of these methods.

A fourth method is referred to in this Recommendation as "manual key exchange".

Manual key exchange is defined as the users entering Key Encryption Keys directly into terminals, without H.234 message exchanges. The same key is entered at both locations. The length of the keys is dependent on the encryption algorithm. The bit order for the keys is most significant bit (MSB) entered first and least significant bit (LSB) entered last. The actual mechanism for entering the keys into the terminal is terminal-dependent and beyond the scope of this Recommendation.

Examples are given below:

- use a telephone keypad to enter: (MSB) 00111010...01110100 (LSB);
- download the same from a computer;
- use a keyboard to enter the same as hexadecimal characters: (MSB) 3A...74 (LSB).

Manual entry may occur prior to initiating the call, or while in a call. In the latter case, the parties may decide to invoke encryption while in a conference, enter a key using the interface provided by the terminal, and then initiate encryption through the terminal's user interface. It is when encryption is requested through the user interface that the BAS code "Encryp-On" is sent, the ECS channel is opened, encryption algorithms are selected, manual mode of key management is agreed to, and session keys are exchanged.

For an encryption system to be regarded as private all conferees should be aware of who/what has access to unencrypted data, whether other conferees or equipment such as MCUs or conversion facilities. This requires an initial set-up period before a conference starts so that entities can authenticate each other. Thus all entities that have access to unencrypted data are identified in an assured manner to all other entities before the conference commences. The authentication framework also provides information to any network provider, for example billing information for an MCU call.

If unencrypted data is available at the MCU (a so-called "trusted MCU") the equipment should be part of any authentication framework. Users should also be made aware that there is a trusted MCU in the network.

Clause 3 deals with aspects common to all methods, while clauses 4, 5 and 6 deal respectively with ISO 8732, Diffie-Hellman, and RSA methods.

## Abbreviations and definitions

**AVSE** Audiovisual Service Entity (terminals, MCUs, etc.)

**\*key\*** Key-encrypting key

## 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.

- ITU-T Recommendation H.221 (1999), *Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices*.
- ITU-T Recommendation H.230 (1999), *Frame-synchronous control and indication signals for audiovisual systems*.
- ITU-T Recommendation H.233 (2002), *Confidentiality system for audiovisual services*.
- ITU-T Recommendation H.242 (1999), *System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s*.
- ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.690 (2002), *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- ISO 8732: 1988, *Banking – Key Management (wholesale)*.
- IETF RFC 2412 (1998), *The Oakley Key Determination Protocol*.

### 3 Message system and key exchange

#### 3.1 Message channel

The system described below consists of a number of defined messages conveyed in sequence between the two ends of the link. The error-free channel required for this purpose is described in ITU-T Rec. H.233, where reference is made to session exchange (SE) blocks.

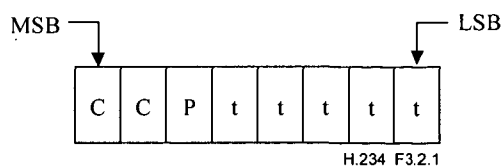
#### 3.2 Message formats

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.690. The length may be encoded in short form or long form. The indefinite form as defined in ITU-T Rec. X.690 will not be used.

A short description of some of the X.690 definitions used within this Recommendation is given below.

##### 3.2.1 Identifier

An identifier is an octet with the structure shown below.



The two bits CC, "Tag Class", define the type of identifier: this is 10 (context specific) for the identifiers defined within this Recommendation.

The Primitive/Constructor (P) bit indicates whether the content is primitive or whether it is composed of nested elements.

The 5-bit Tag (ttttt) uniquely defines the identifier (according to its class).

Thus, all identifiers in this Recommendation have the octet form: 1 0 P t<sub>1</sub> t<sub>2</sub> t<sub>3</sub> t<sub>4</sub> t<sub>5</sub>.