

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.3

(09/2005)

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

H.323 security: Hybrid security profile

ITU-T Recommendation H.235.3

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.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
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
BROADBAND AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619

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

ITU-T Recommendation H.235.3

H.323 security: Hybrid security profile

Summary

The purpose of this Recommendation is to describe an efficient and scalable, PKI-based hybrid security profile for version 2 or higher of ITU-T Rec. H.235.0. The hybrid security profile contained herein takes advantage of the security profiles in ITU-T Recs H.235.1 and H.235.2 by deploying digital signatures from ITU-T Rec. H.235.2 and deploying the baseline security profile from ITU-T Rec. H.235.1.

In earlier versions of the H.235 sub-series, this profile was contained in Annex F/H.235. Appendices IV, V, VI to H.235.0 show the complete clause, figure, and table mapping between H.235 versions 3 and 4.

Source

ITU-T Recommendation H.235.3 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Authentication, certificate, digital signature, encryption, integrity, key management, multimedia security, security profile.

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.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

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 2006

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	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	2
3	Terms and definitions	2
4	Symbols and abbreviations	2
5	Conventions	3
6	Overview	4
6.1	H.323 requirements	6
6.2	Authentication and integrity	7
7	Procedure IV	7
8	Security association for concurrent calls	9
9	Key update	10
10	Usage of elliptic curve techniques	11
11	Illustration examples.....	11
12	Multicast behaviour	14
13	List of secure signalling messages.....	14
13.1	H.225.0 RAS	14
13.2	H.225.0 call signalling (single administrative domain).....	14
13.3	H.225.0 call signalling (multi-administrative domain)	15
14	List of object identifiers.....	15
	Appendix I – H.235.3 enabled Gatekeeper Security Processor	16
I.1	Discovery of a gatekeeper security processor	18
I.2	Gatekeeper security processor operation.....	19
I.3	Processor token.....	20
I.4	GKSP illustration example	23
I.5	List of object identifiers.....	28

ITU-T Recommendation H.235.3

H.323 security: Hybrid security profile

1 Scope

The purpose of this Recommendation is to describe an efficient and scalable, PKI-based hybrid security profile for version 2 and higher of ITU-T Rec. H.235.0. The hybrid security profile contained herein takes advantage of the security profiles in ITU-T Recs H.235.1 and H.235.2 by deploying digital signatures from ITU-T Rec. H.235.2 and deploying the baseline security profile from ITU-T Rec. H.235.1.

2 References

2.1 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.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- ITU-T Recommendation H.235, version 1 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.
- ITU-T Recommendation H.235, version 2 (2000), *Security and encryption for H-series (H.323 and other H.245-Based) multimedia terminals*.
- ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.
- ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.
- ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile*.
- ITU-T Recommendation H.235.6 (2005), *H.323 security: Voice encryption profile with native H.235/H.245 key management*.
- ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.
- ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.
- ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.
- ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

2.2 Informative references

- [ISO|IEC 14888-3] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix; Part 3: Certificate-based mechanisms*.
- [PKCS] PKCS #1 v2.0: *RSA Cryptography Standard*; RSA Laboratories; October 1, 1998; <http://www.rsa.com/rsalabs/pubs/PKCS/index.html>.
- [PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; <http://www.rsa.com/rsalabs/pubs/PKCS/index.html>.
- [RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.

3 Terms and definitions

For the purposes of this Recommendation, the definitions given in clauses 3/H.323, 3/H.225.0 and 3/H.245 apply. Some of the terms used in this Recommendation are also as defined in ITU-T Recs X.800 | ISO 7498-2, X.803 | ISO/IEC 10745, X.810 | ISO/IEC 10181-1, X.811 | ISO/IEC 10181-2 and H.235.0.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

ALG	Application Level Gateway
ASN.1	Abstract Syntax Notation One
BRJ	Bandwidth Reject
BRQ	Bandwidth Request
CA	Certification Authority
CRL	Certificate Revocation List
DB	Database
DH	Diffie-Hellman
DN	Distinguished Name
EP	Endpoint
GCF	Gatekeeper Confirm
GK	Gatekeeper
GKID	Gatekeeper Identifier
GKSP	Gatekeeper Security Processor

GRJ	Gatekeeper Reject
GRQ	Gatekeeper Request
HMAC	Hashed Message Authentication Code
ICV	Integrity Check Value
ID	Identifier
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LRQ	Location Request
MCU	Multipoint Control Unit
MD5	Message Digest 5
NAT	Network Address Translation
OID	Object Identifier
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
RAS	Registration, Admission and Status
RCF	Registration Confirm
RRJ	Registration Reject
RRQ	Registration Request
RSA	Rivest, Shamir and Adleman encryption algorithm
RTP	Real-time Transport Protocol
SHA	Secure Hash Algorithm
UDP	User Datagram Protocol
URQ	Unregistration Request
VoIP	Voice-over-IP

5 Conventions

In this Recommendation the following conventions are used:

- "shall" indicates a mandatory requirement.
- "should" indicates a suggested but optional course of action.
- "may" indicates an optional course of action rather than a recommendation that something take place.

The hybrid security profile uses terms and definitions from ITU-T Recs H.235.1 and H.235.2.

While the message integrity service always provides message authentication, the reverse is not always true. For the authentication-only mode, the integrity assured only spans a certain subset of message fields. This applies to integrity services realized by asymmetric means (e.g., digital signatures). Thus, in practice, a combined authentication and integrity service uses the same key material without introducing a security weakness.

This security profile is applicable in environments with potentially many terminals, where static password/symmetric key assignment is not feasible, e.g., in large-scale or global-scale scenarios.

Instead, this security profile assumes availability of a public-key infrastructure with assigned certificates and private/public-keys, directories, etc. In addition, this security profile deploys symmetric crypto techniques where applicable.

This security profile introduces the terms "first" message and "last" message sent. Security protection of the first message (and probably also for the last message) is different from security protection of the remaining other messages.

The "first message" sent is understood as a message that flows between two H.323 entities and establishes a security context. It makes symmetric key material available to both entities and, for example, marks the beginning of a call. For H.225.0 RAS, the first message is the RRQ and the related response message. For H.225.0 call signalling using fast start, the first message is SETUP and CONNECT.

The "last message" terminates the established security context. The established key material shall be destroyed. For H.225.0 RAS, the last message is the URQ and related response message, while for H.225.0 call signalling the last message is RELEASE-COMPLETE.

6 Overview

This Recommendation describes an efficient and scalable, PKI-based hybrid security profile deploying digital signatures from H.235.2 and deploying the baseline security profile from H.235.1. This Recommendation is suggested as an option. H.323 security entities (terminals, gatekeepers, gateways, MCUs, etc.) may implement this hybrid security profile for improved security or whenever required.

The notion of "hybrid" in this text shall mean that security procedures from the signature profile in ITU-T Rec. H.235.2 are actually applied in a lightweight sense and the digital signatures still conform to the RSA procedures. However, digital signatures are deployed only where absolutely necessary while highly efficient symmetric security techniques from the baseline security profile in ITU-T Rec. H.235.1 are used otherwise.

The hybrid security profile is applicable for scaleable "global" IP telephony. This security profile overcomes the limitations of the simple, baseline security profile of H.235.1 when strictly applying it. Furthermore, this security profile overcomes certain drawbacks of H.235.2, such as the need for higher bandwidth and increased performance needs for processing, when strictly applying it. For example, the hybrid security profile does not depend on the (static) administration of mutual shared secrets of the hops in different domains. Thus, users can more easily choose their VoIP provider. This security profile thus supports a certain kind of user mobility as well. It applies asymmetric cryptography with signatures and certificates only where necessary and otherwise uses simpler and more efficient symmetric techniques. It provides tunnelling of H.245 messages for H.245 message integrity and also implements some provisions for non-repudiation of messages.

The hybrid security profile mandates the GK-routed model and is based upon the H.245 tunnelling techniques. Support for non GK-routed models is for further study.

The features provided by this profile include:

For RAS, H.225.0 and H.245 messages:

- User authentication to a desired entity irrespective of the number of application level hops that the message traverses.
NOTE 1 – Hop is understood here in the sense of a trusted H.235 network element (e.g., GK, GW, MCU, proxy, or firewall). Thus, application level hop-by-hop security when used with symmetric techniques does not provide true end-to-end security between terminals.
- Integrity of all or critical portions (fields) of messages arriving at an entity irrespective of the number of application-level hops that the message traverses. Integrity of the message itself using a strongly generated random number is also optional.
- Application-level hop-by-hop message authentication, integrity and (some) non-repudiation provide these security services for the entire message.
- Using the available public-key infrastructure, users can choose their service provider. Key-management for session key distribution is well integrated in the hybrid security profile.

Suitable provision of the above-described security services thwarts several types of attacks, including:

- *Man-in-the-middle attacks*: Application-level hop-by-hop message authentication and integrity prevents against such attacks when the man-in-the-middle is in an application-level hop, say, a hostile router.
- *Replay attacks*: Use of timestamps and sequence numbers prevent such attacks.
- *Spoofing*: User authentication prevents such attacks.
- *Connection hijacking*: Use of authentication/integrity for each signalling message prevents such attacks.

This security profile assumes the GK-routed call model, where the fast connect call signalling method is applied. H.245 call control messages are securely tunnelled in H.225.0 call signalling messages and inherit thereby the H.225.0 security protection scheme.

The signature security profile allows to securely tunnel H.245 call control PDUs within H.225.0 facility messages. The H.245 key update and synchronization mechanisms require tunnelling for key-update FACILITY message to be signalled and is useful, for example, for very long duration calls.

The diagonally shaded area in Table 1 represents the security mechanisms that are used by the hybrid security profile.

NOTE 2 – RSA certificates with MD5 ([RFC1321]) hashing are not part of this security profile.

The voice encryption security profile of H.235.6 (see 6.1/H.235.6) could be optionally used in conjunction with the hybrid security profile. Its use is negotiated as part of the call set-up signalling.