

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.235.1

(09/2005)

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

H.323 security: Baseline security profile

ITU-T Recommendation H.235.1

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.235.1

H.323 security: Baseline security profile

Summary

This Recommendation provides authentication and integrity protection, or authentication-only for H.225.0 RAS and call signalling, H.225.0, and tunnelled H.245 using password-based HMAC-SHA1-96 hash protection of H.225.0 RAS and Call Signalling messages by using secure password-based cryptographic techniques. The security profile is applicable to H.323 terminal-to-gatekeeper, gatekeeper-to-gatekeeper, H.323 gateway-to-gatekeeper and to other H.323 entities in administered environments with symmetric assigned keys/passwords.

In earlier versions of the H.235 subseries, this profile was contained in Annex D/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.235.1 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 not 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	5
6.1	Summary of security features.....	5
6.2	Applicability of the baseline security profile	6
6.3	H.323 requirements	7
6.4	Overview of procedures	7
7	Symmetric-key-based signalling message authentication and integrity (procedure I)	7
7.1	Computation of the password-based hash	9
7.2	HMAC-SHA1-96	9
7.3	Computation and verification of authentication and integrity.....	9
8	Authentication-only (procedure IA)	10
9	Usage illustration for procedure I	11
9.1	RAS message authentication and integrity.....	13
9.2	H.225.0 message authentication and integrity.....	13
9.3	H.245 message authentication and integrity.....	14
9.4	Direct-routed scenario	15
10	Back-end-service support	15
11	H.235 version 1 compatibility	15
12	Multicast behaviour	15
13	List of secured signalling messages.....	15
13.1	H.225.0 RAS	15
13.2	H.225.0 call signalling.....	15
13.3	H.245 call control	16
14	Usage of sendersID and generalID	16
15	List of object identifiers.....	17



Documents

ITU-T Rec. H.235.1 (09/2005)

Document Sharing Hub

iii

ITU-T Recommendation H.235.1

H.323 Security: Baseline security profile

1 Scope

This Recommendation provides authentication and integrity protection, or authentication-only for H.225.0 RAS and call signalling, H.225.0 and tunnelled H.245 messages using password-based HMAC-SHA1-96 hash protection of H.225.0 RAS and Call Signalling messages by using secure password-based cryptographic techniques. The security profile is applicable to H.323 terminal-to-gatekeeper, gatekeeper-to-gatekeeper, H.323 gateway-to-gatekeeper and to other H.323 entities.

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.235.2 (2005), *H.323 security: Signature security profile*.
- ITU-T Recommendation H.235.4 (2005), *H.323 security: Direct and selective routed call security*.
- 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 version 10 (2003), *Control protocol for multimedia communication*.
- ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.
- ITU-T Recommendation H.323 Annex F (1999), *Simple endpoint types*.
- ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

ISO/IEC 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*.
- ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

2.2 Informative references

- [FIPSPUB180-2] Federal Information Processing Standard FIPS PUB 180-2, Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.
- [OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.
- [RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.
- [WEBOIDs] <http://www.alvestrand.no/objectid/top.html>.

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 along with those in this clause. Some of the terms used in this Recommendation are also as defined in ITU-T Recs X.800 | ISO/IEC 7498-2, X.803 | ISO/IEC 10745, X.810 | ISO/IEC 10181-1 and X.811 | ISO/IEC 10181-2.

This Recommendation uses the following terms for provisioning the security services.

3.1 authentication and integrity: This is a combined security service part of the baseline profile that supports message integrity in conjunction with user authentication. The user may ensure authentication by correctly applying a shared secret key procedure. Both security services are provided by the same security mechanism.

3.2 authentication-only: This security service offered by the baseline security profile as an option supports authentication of selected fields only, but does not provide full message integrity. The authentication-only security profile is applicable for signalling messages traversing NAT/firewall devices. The user may ensure authentication by correctly applying a shared secret key procedure.

When using symmetric key techniques, the security services authentication/integrity only apply on a hop-by-hop basis.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

- | | |
|-------|------------------------------|
| ASN.1 | Abstract Syntax Notation One |
| EP | Endpoint |
| EPID | Endpoint Identifier |