

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.235.2

(09/2005)

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

H.323 security: Signature security profile

ITU-T Recommendation H.235.2

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.235.2

H.323 security: Signature security profile

Summary

This Recommendation describes an optional security profile for deploying digital signatures to secure the H.225.0 signalling.

In earlier versions of the H.235 subseries, this profile was contained in Annex E/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.235.2 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	3
5	Conventions	4
6	Overview	5
6.1	H.323 requirements	7
7	Digital signatures with public/private key pairs details (procedure II)	8
8	Multipoint conferencing procedures.....	9
9	End-to-end authentication (procedure III).....	9
10	Authentication-only	11
11	Authentication and integrity	12
12	Computation of the digital signature	12
13	Verification of the digital signature	13
14	Handling of certificates.....	13
15	Usage illustration for procedure II.....	15
15.1	RAS message authentication, integrity and non-repudiation	15
15.2	RAS authentication only.....	16
15.3	H.225.0 message authentication, integrity and non-repudiation	17
15.4	H.245 message authentication and integrity.....	17
16	H.235 version 1 compatibility	18
17	Multicast behaviour	18
18	List of secure signalling messages.....	18
18.1	H.225.0 RAS	18
18.2	H.225.0 call signalling.....	19
19	Usage of sendersID and generalID	19
20	List of object identifiers.....	20

ITU-T Recommendation H.235.2

H.323 security: Signature security profile

1 Scope

This Recommendation describes an optional security profile for deploying digital signatures to secure the H.225.0 signalling.

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 (1998), *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.235.6 (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*.
- 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 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.
- 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*.
- [RFC3447] IETF RFC 3447 (2003), *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

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 defined in ITU-T Recs X.800 | ISO 7498-2, X.803 | ISO/IEC 10745, X.810 | ISO/IEC 10181-1 and X.811 | ISO/IEC 10181-2.

3.1 certification authorities: Certification Authorities (CAs), when used in the context of electronic signature, certify public verification keys by issuing "Certificates".

3.2 certificate repositories: Certificate repositories (e.g., an X.500 Directory) hold user certificates and Certificate Revocation Lists (CRLs). They are trusted to make that information accessible but are not responsible for the content or accuracy of the information they receive from the CAs or the RAs.

3.3 digital signature: Is a cryptographic transformation (using an asymmetric cryptographic technique) of the numerical representation of a data message, such that any person having the signed message and the relevant public key can determine that:

- the transformation was created using the private key corresponding to the relevant public key; and
- the signed message has not been altered since the cryptographic transformation.

3.4 on-line certificate status providers: The On-line Certificate Status Protocol (OCSP) enables applications to determine the revocation state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing revocation information in a more timely way than is possible with CRLs. On-line certificate status providers can be seen as an alternative to the use of off-line CRLs.

3.5 proxy: The proxy is an intermediate H.323 entity similar to a gatekeeper. The proxy may be a separate network node or may be collocated with the functionality of an H.323 entity such as of the gatekeeper. The proxy may perform security tasks such as signature and certificate verification and access control.

3.6 registration authorities: Registration authorities act as intermediaries between users and CAs. They receive requests from users and transmit them to the CAs in an appropriate form.

3.7 time stamping authorities: Time stamping authorities are mandatory for non-repudiation in case of key loss or key compromise. In practice, they provide a counter-signature to anyone, including a reliable time, over a hash and a hash identifier.

3.8 trust service provider: An entity, which can be used by other entities as a trusted intermediary in a communication or verification process, or as a trusted information service provider.

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

3.9 authentication-only: This security service of the signature security profile supports user authentication where the user authenticates when correctly digitally signing some piece of data by the private key. Note that this security service does not provide countermeasures against arbitrary cut and paste, message manipulation or tampering attacks. Authentication-only may be useful for security proxies that verify authenticity of the message (data origin authentication) when forwarding the message to another destination (e.g., Gatekeeper).

NOTE – The forwarding usually changes certain parts of the message; thus end-to-end integrity cannot be realized.

Nevertheless, authentication-only can be applied on a hop-by-hop basis as well. Procedure III specifies this security service for an end-to-end scenario while procedure II specifies this security service for the hop-by-hop case.

3.10 authentication and integrity: This is a combined security service that supports message integrity in conjunction with user authentication. The user authenticates when correctly digitally signing some piece of data by the private key. In addition to that, the message is protected against tampering. Both security services are provided by the same security mechanism. Combined authentication and integrity is possible only on a hop-to-hop basis. Procedure II specifies this security service.

NOTE – When digital signatures are applied, a non-repudiation security service may be supported; this depends also on the settings of the key usage bits of the signing key in the certificate (see also RFC 3280).

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

ARQ	Admission Request
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CRL	Certificate Revocation List
DH	Diffie-Hellman
DNS	Domain Name Service
EP	Endpoint
EPID	Endpoint Identifier
GK	Gatekeeper
GKID	Gatekeeper Identifier
GRQ	Gatekeeper Request
ICV	Integrity Check Value
IP	Internet Protocol
ITU	International Telecommunication Union