

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.235.0

(01/2014)

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

H.323 security: Framework for security in ITU-T H-series (ITU-T H.323 and other ITU-T H.245-based) multimedia systems

Recommendation ITU-T H.235.0

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, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Interoperability compliance testing of personal health systems (HRN, PAN, LAN and WAN)	H.820–H.849
Multimedia e-health data exchange services	H.860–H.869

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

Recommendation ITU-T H.235.0

H.323 security: Framework for security in ITU-T H-series (ITU-T H.323 and other ITU-T H.245-based) multimedia systems

Summary

Recommendation ITU-T H.235.0 describes enhancements within the framework of the ITU-T H.3xx-series of Recommendations to incorporate security services such as authentication and privacy (data encryption). The proposed scheme is applicable to both simple point-to-point and multipoint conferences for any terminals which utilize Recommendation ITU-T H.245 as a control protocol and also to ITU-T H.323 systems that use the ITU-T H.225.0 RAS and/or call signalling protocol.

For example, ITU-T H.323 systems operate over packet-based networks which do not provide a guaranteed quality of service (QoS). For the same technical reasons that the base network does not provide QoS, the network does not provide a secure service. Secure real-time communication over insecure networks generally involves two major areas of concern – authentication and privacy.

This Recommendation describes the security infrastructure and specific privacy techniques to be employed by the ITU-T H.3xx-series of multimedia systems. This Recommendation covers areas of concern for interactive conferencing. These areas include, but are not strictly limited to, authentication and privacy of all real-time media streams that are exchanged in the conference. This Recommendation provides the protocol and algorithms needed between the ITU-T H.323 entities.

This Recommendation utilizes the general facilities supported in Recommendation ITU-T H.245 and as such, any standard which operates in conjunction with this control protocol may use this security framework. It is expected that wherever possible, other ITU-T H-series terminals may interoperate and directly utilize the methods described in this Recommendation. This Recommendation will not initially provide for complete implementation in all areas and will specifically highlight end-point authentication and media privacy.

This Recommendation includes the ability to negotiate services and functionality in a generic manner and to be selective concerning cryptographic techniques and capabilities utilized. The specific manner in which they are used relates to systems capabilities, application requirements and specific security policy constraints. This Recommendation supports varied cryptographic algorithms, with varied options appropriate for different purposes (e.g., key lengths). Certain cryptographic algorithms may be allocated to specific security services (e.g., one for fast media stream encryption and another for signalling encryption).

It should also be noted that some of the available cryptographic algorithms or mechanisms may be reserved for export or other national issues (e.g., with restricted key lengths). This Recommendation supports signalling of well-known algorithms in addition to signalling non-standardized or proprietary cryptographic algorithms. There are no specifically mandated algorithms; however, it is strongly suggested that end points support as many of the applicable algorithms as possible in order to achieve interoperability. This parallels the concept that the support of Recommendation ITU-T H.245 does not guarantee the interoperability between two entities' codecs.

Version 4 of Recommendation ITU-T H.235 broke up Recommendation ITU-T H.235 version 3 into a suite of ITU-T H.235.x sub-series Recommendations, and restructures the sub-series. Recommendations ITU-T H.235.8 and ITU-T H.235.9 were added to the suite, other sub-series Recommendations have been extended with new functionality (Recommendations ITU-T H.235.3 and ITU-T H.235.5). Recommendation ITU-T H.235.0 contains the ITU-T H.323 security framework with common text and useful general information for all ITU-T H.235.x sub-series Recommendations.

Appendices IV, V and VI provide a mapping of text, figures and tables from Recommendation ITU-T H.235 version 3 (2003), including the subsequent Corrigendum 1 and amendments to the new structure.

This revision of Recommendation ITU-T H.235.0 is an enhancement to version 4 to add support for key material with lengths exceeding 2048 bits.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.235.0	2005-09-13	16	11.1002/1000/8592-en
2.0	ITU-T H.235.0	2014-01-13	16	11.1002/1000/12058-en

Keywords

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

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2014

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

Table of Contents

		Page
1	Scope	1
1.1	Structure of ITU-T H.235.x sub-series Recommendations	2
2	References.....	2
3	Terms and definitions	4
3.1	Terms defined elsewhere	4
3.2	Terms defined in this Recommendation.....	5
4	Abbreviations and acronyms	6
5	Conventions	7
6	System introduction.....	8
6.1	Summary.....	9
6.2	Authentication	9
6.3	Call establishment security.....	10
6.4	Call control (ITU-T H.245) security	10
6.5	Media stream privacy	10
6.6	Trusted elements.....	11
6.7	Non-repudiation.....	11
6.8	Mobility security	11
6.9	Security profiles.....	12
6.10	Secured NAT/firewall traversal.....	12
7	Connection establishment procedures	13
8	Authentication signalling and procedures	13
8.1	Diffie-Hellman with optional authentication.....	13
8.2	Subscription-based authentication.....	14
8.3	RAS signalling/procedures for authentication.....	18
8.4	Key management on the RAS channel.....	21
9	Asymmetric authentication and key exchange using elliptic curve crypto systems.....	21
9.1	Key management	22
9.2	Digital signature	22
10	Pseudo-random function (PRF)	22
11	Security error recovery	23
11.1	Error signalling.....	23
	Annex A – ITU-T H.235 ASN.1	25
	Annex B – ITU-T H.324-specific topics.....	31
	Appendix I – ITU-T H.323 implementation details.....	32
	I.1 Implementation examples.....	32
	Appendix II – ITU-T H.324 implementation details	38

	Page
Appendix III – Other ITU-T H-series implementation details	39
Appendix IV – Section mapping of ITU-T H.235v3Amd1Cor1 to ITU-T H.235v4 sub-series Recommendations	40
Appendix V – Figure mapping of ITU-T H.235v3Amd1Cor1 to ITU-T H.235v4 sub-series Recommendations	49
Appendix VI – Table mapping of ITU-T H.235v3Amd1Cor1 to ITU-T H.235v4 sub-series Recommendations	52
Bibliography.....	53

Document ID: 123456789

Recommendation ITU-T H.235.0

ITU-T H.323 security: Framework for security in ITU-T H-series (ITU-T H.323 and other ITU-T H.245-based) multimedia systems

1 Scope

The primary purpose of Recommendation ITU-T H.235.0 is to provide a security framework for authentication, privacy and integrity within the current ITU-T H-series protocol framework. The current text of this Recommendation provides details on implementation with [ITU-T H.323]. This framework is expected to operate in conjunction with other ITU-T H-series protocols that utilize [ITU-T H.245] as their control protocol and/or use the ITU-T H.225.0 RAS and/or call signalling protocol.

Additional goals in this Recommendation include:

- 1) Security architecture should be developed as an extensible and flexible framework for implementing a security system for ITU-T H-series terminals and other ITU-T H.323-based systems. This should be provided through flexible and independent services and the functionality that they supply. This includes the ability to negotiate and to be selective concerning the cryptographic techniques utilized and the manner in which they are used.
- 2) Provide security for all communications occurring as a result of ITU-T H.3xx protocol usage. This includes aspects of connection establishment, call control and media exchange between all entities. This requirement includes the use of confidential communication (privacy) and may exploit functions for peer authentication, as well as protection of the user's environment from attacks.
- 3) This Recommendation should not preclude integration of other security functions in ITU-T H.3xx entities which may protect them against attacks from the network.
- 4) This Recommendation should not limit the ability for any ITU-T H.3xx-series Recommendation to scale as appropriate. This may include both the number of secured users and the levels of security provided.
- 5) Where appropriate, all mechanisms and facilities should be provided independent of any underlying transport or topologies. Other means that are outside the scope of this Recommendation may be required to counter such threats.
- 6) Provisions are made for operation in a mixed environment (secured and unsecured entities).
- 7) This Recommendation should provide facilities for distributing session keys associated with the cryptography utilized. (This does not imply that public-key-based certificate management must be part of this Recommendation.)
- 8) This Recommendation provides two security profiles that facilitate interoperability. [ITU-T H.235.1] describes a simple, yet secure password-based security profile while [ITU-T H.235.2] is a signature security profile deploying digital signatures, certificates and a public-key infrastructure that overcomes the limitations of [ITU-T H.235.1].

The security architecture described in this Recommendation, does not assume that the participants are familiar with each other. It does, however, assume that appropriate precautions have been taken to physically secure the ITU-T H-series end points. The principal security threat to communications therefore is assumed to be eavesdropping on the network, or some other method of diverting media streams.

[ITU-T H.323] provides the means to conduct an audio, video and data conference between two or more parties, but does not provide the mechanism to allow each participant to authenticate the

identity of the other participants, nor provide the means to make the communications private (i.e., encrypt the streams).

[ITU-T H.323], [ITU-T H.324] and [ITU-T H.310] make use of the logical channel signalling procedures of [ITU-T H.245], in which the content of each logical channel is described when the channel is opened. Procedures are provided for expression of receiver and transmitter capabilities, transmissions are limited to what receivers can decode and receivers may request a particular desired mode from transmitters. The security capabilities of each end point are communicated in the same manner as any other communication capability.

Some ITU-T H-series [ITU-T H.323] terminals may be used in multipoint configurations. The security mechanism described in this Recommendation will allow for secure operation in these environments, including both centralized and decentralized MCU operation.

1.1 Structure of ITU-T H.235.x sub-series Recommendations

This security framework Recommendation encompasses the following structure within the ITU-T H.235.x sub-series of Recommendations, as shown in Figure 1. This Recommendation contains common text and useful general information for all ITU-T H.235.x sub-series Recommendations.

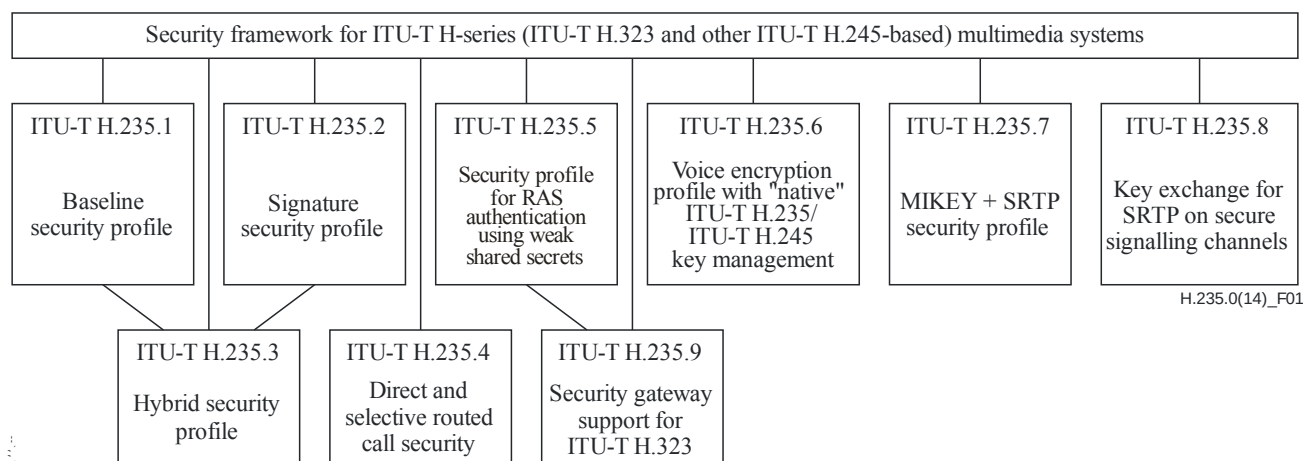


Figure 1 – Structure of ITU-T H.235.x sub-series Recommendations

The vertical lines in Figure 1 indicate direct dependencies from the main text, [ITU-T H.235.0], there may be more indirect dependencies from other ITU-T H.235.x Recommendations. Several Recommendations could be used in combination and complementarily; see also clause 6.9.

2 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 H.225.0] Recommendation ITU-T H.225.0 v7 (2009), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

- [ITU-T H.235] Recommendation ITU-T H.235 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.*
- [ITU-T H.235.1] Recommendation ITU-T H.235.1 (2005), *H.323 security: Baseline security profile.*
- [ITU-T H.235.2] Recommendation ITU-T H.235.2 (2005), *H.323 security: Signature security profile.*
- [ITU-T H.235.3] Recommendation ITU-T H.235.3 (2005), *H.323 security: Hybrid security profile.*
- [ITU-T H.235.4] Recommendation ITU-T H.235.4 (2005), *H.323 security: Direct and selective routed call security.*
- [ITU-T H.235.5] Recommendation ITU-T H.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets.*
- [ITU-T H.235.6] Recommendation ITU-T H.235.6 (2014), *H.323 security: Encryption profile with native ITU-T H.235/H.245 key management.*
- [ITU-T H.235.7] Recommendation ITU-T H.235.7 (2005), *H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235.*
- [ITU-T H.235.8] Recommendation ITU-T H.235.8 (2005), *H.323 security: Key exchange for SRTP using secure signalling channels.*
- [ITU-T H.235.9] Recommendation ITU-T H.235.9 (2005), *H.323 security: Security gateway support for H.323.*
- [ITU-T H.245] Recommendation ITU-T H.245 v16 (2011), *Control protocol for multimedia communication.*
- [ITU-T H.323] Recommendation ITU-T H.323 v7 (2009), *Packet-based multimedia communications systems.*
- [ITU-T H.324] Recommendation ITU-T H.324 (2009), *Terminal for low bit-rate multimedia communication.*
- [ITU-T H.510] Recommendation ITU-T H.510 (2002), *Mobility for H.323 multimedia systems and services.*
- [ITU-T H.530] Recommendation ITU-T H.530 (2002), *Symmetric security procedures for H.323 mobility in H.510.*
- [ITU-T Q.931] Recommendation ITU-T Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control.*
- [ITU-T X.800] Recommendation ITU-T X.800 (1991) | ISO/IEC 7498-2:1989, *Security architecture for Open Systems Interconnection for CCITT applications.*
- [ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model.*
- [ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*
- [ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*
- [IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0.*

[IETF RFC 2401]	IETF RFC 2401 (1998), <i>Security Architecture for the Internet Protocol</i> .
[IETF RFC 2407]	IETF RFC 2407 (1998), <i>The Internet IP Security Domain of Interpretation for ISAKMP</i> .
[IETF RFC 2408]	IETF RFC 2408 (1998), <i>Internet Security Association and Key Management Protocol (ISAKMP)</i> .
[IETF RFC 2865]	IETF RFC 2865 (2000), <i>Remote Authentication Dial In User Service (RADIUS)</i> .
[IETF RFC 3546]	IETF RFC 3546 (2003), <i>Transport Layer Security (TLS) Extensions</i> .
[IETF RFC 3830]	IETF RFC 3830 (2004), <i>MIKEY: Multimedia Internet KEYing</i> .
[ISO 7498-2]	ISO 7498-2:1989, <i>Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture</i> .
[ISO/IEC 9798-2]	ISO/IEC 9798-2:2008, <i>Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms</i> .
[ISO/IEC 9798-3]	ISO/IEC 9798-3:1998, <i>Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques</i> .
[ISO/IEC 9798-4]	ISO/IEC 9798-4:1999, <i>Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function</i> .
[ISO/IEC 14888-3]	ISO/IEC 14888-3:2006, <i>Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms</i> .
[ISO/IEC 15946-1]	ISO/IEC 15946-1:2008, <i>Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General</i> .
[af-sec-0100.002]	af-sec-0100.002 (2001), <i>ATM Security Specification Version 1.1</i> , ATM Forum.

3 Terms and definitions

For the purposes of this Recommendation, the definitions given in clause 3 of [ITU-T H.323], [ITU-T H.225.0] and [ITU-T H.245] apply along with those listed in clause 3.1. Some of the following terms used in this Recommendation are also defined in [ITU-T X.800], [ITU-T X.803], [ITU-T X.810] and [ITU-T X.811].

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [ITU T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.3 key management [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.4 symmetric (secret-key based) cryptographic algorithm [ITU-T X.810]: An algorithm for performing encipherment or the corresponding algorithm for performing decipherment in which the same key is required for both encipherment and decipherment.

3.1.5 threat [ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authorization: The granting of permission on the basis of authenticated identification.

3.2.2 attack: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.

3.2.3 certificate: A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data, see [ITU-T X.810]. In this Recommendation, the term refers to "public key" certificates which are values that represent an owner's public key (and other optional information) as verified and signed by a trusted authority in an unforgeable format.

3.2.4 cipher: A cryptographic algorithm, a mathematical transform.

3.2.5 confidentiality: The property that prevents disclosure of information to unauthorized individuals, entities or processes.

3.2.6 cryptographic algorithm: Mathematical function that computes a result from one or several input values.

3.2.7 EC-GDSA: Elliptic curve digital signature with appendix analogue of the NIST digital signature algorithm (DSA); see also clause 6.6 of [ISO/IEC 14888-3].

3.2.8 elliptic curve cryptosystem: A public-key cryptosystem (see section 8.7 of [af-sec-0100.002]).

3.2.9 elliptic curve key agreement scheme – Diffie-Hellman: The Diffie-Hellman key agreement scheme using elliptic curve cryptography.

3.2.10 encipherment: Encipherment (encryption) is the process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an encryption algorithm). Decipherment (decryption) is the reverse operation by which ciphertext is transformed to plaintext.

3.2.11 integrity: The property that data has not been altered in an unauthorized manner.

3.2.12 media stream: A media stream can be of type audio, video or data or a combination of any of them. Media stream data conveys user or application data (payload) but no control data.

3.2.13 non-repudiation: Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.2.14 privacy: A mode of communication in which only the explicitly enabled parties can interpret the communication. This is typically achieved by encryption and shared key(s) for the cipher.

3.2.15 private channel: For this Recommendation, a private channel is one that is a result of prior negotiation on a secure channel. In this context, it may be used to handle media streams.

3.2.16 public-key cryptography: An encryption system utilizing asymmetric keys (for encryption/decryption) in which the keys have a mathematical relationship to each other which cannot be reasonably calculated.

3.2.17 security profile: A (sub)set of consistent, interoperable procedures and features from [ITU-T H.235] which is useful for securing ITU-T H.323 multimedia communication among the involved entities in a specific scenario.

3.2.18 spamming: A denial-of-service attack when sending unauthorized data in excess to a system. A special case is media spamming when sending RTP packets on UDP ports. Usually the system is flooded with packets, the processing of which consumes precious system resources.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3DES	Triple Data Encryption Standard algorithm
AES	Advanced Encryption Standard algorithm
ALG	Application Layer Gateway
ASN.1	Abstract Syntax Notation One
BES	Back-End Server
CA	Certificate Authority
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CRL	Certificate Revocation List
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name System
DSS	Digital Signature Standard
DTMF	Dual Tone Multi-Frequency
ECB	Electronic Code Book
ECC / EC	Elliptic Curve Cryptosystem
EC-GDSA	Elliptic Curve digital signature with appendix analogue of the NIST Digital Signature Algorithm (DSA)
ECKAS-DH	Elliptic Curve Key Agreement Scheme – Diffie-Hellman
EOFB	Enhanced OFB mode
EP	End Point
GK	Gatekeeper
GW	Gateway
ICV	Integrity Check Value
ID	Identifier
IPsec	Internet Protocol security
ISAKMP	Internet Security Association Key Management Protocol
IV	Initialization Vector
LDAP	Lightweight Directory Access Protocol

MAC	Message Authentication Code
MC	Multipoint Controller
MCU	Multipoint Control Unit
MPS	Multiple Payload Stream
NAT	Network Address Translation
OCSF	Online Certificate Status Protocol
OFB	Output Feedback Mode
OID	Object Identifier
PDU	Protocol Data Unit
PKI	Public-Key Infrastructure
POTS	Plain Old Telephone Service
PRF	Pseudo-Random Function
Q&A	Question and Answer
QoS	Quality of Service
RAS	Registration, Admission and Status
RSA	Rivest, Shamir and Adleman (public-key algorithm)
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SA	Security Association
SASET	Secure Audio Simple End-point Type
SDU	Service Data Unit
SHA1	Secure Hash Algorithm 1
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSAP	Transport Service Access Point
TTP	Trusted Third Party
UDP	User Datagram Protocol
XOR, $\oplus$	Exclusive OR
X Y	Concatenation of X and Y

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.

References to clauses, subclauses, annexes and appendices refer to those items within this Recommendation unless another Recommendation is explicitly listed. For example, "1.4" refers to clause 1.4 of this Recommendation; "6.4/H.245" refers to clause 6.4 of [ITU-T H.245].

This Recommendation describes the use of "n" different message types: ITU-T H.245, RAS, ITU-T Q.931, etc. To distinguish between the different message types, the following convention is followed. ITU-T H.245 message and parameter names consist of multiple concatenated words highlighted in bold typeface (**maximumDelayJitter**). RAS message names are represented by three-letter abbreviations (**ARQ**). ITU-T Q.931 message names consist of one or two words with the first letters capitalized (**Call Proceeding**).

This Recommendation uses the notion of setting a compound ASN.1 data structure to NULL, for example, "**paramS** set to NULL" (see clause 7 of [ITU-T H.235.1], clause 8 of [ITU-T H.235.1], clause 9.1 of [ITU-T H.235.1], clause 9.2 [ITU-T H.235.1], clause 7 of [ITU-T H.235.2], clause 9 of [ITU-T H.235.2], clause 15.1 of [ITU-T H.235.2] and clause 15.2 of [ITU-T H.235.2]). This shall mean that all optional elements in the particular SEQUENCE (i.e., **Params**) are absent.

This Recommendation defines various object identifiers (OIDs) for signalling security capabilities, procedures or security algorithms. These OIDs relate to a hierarchical tree of assigned values that may originate from external sources, or are part of the ITU-T maintained OID tree. Those OIDs that are specifically related to [ITU-T H.235] have the following appearance in the text:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V** **N**} where **V** symbolically represents a single decimal digit denoting the corresponding version of [ITU-T H.235]; e.g., 1, 2, 3 or 4. **N** symbolically represents a decimal number uniquely identifying the instance of the OID and thus, the procedure, algorithm or security capability.

Thus, the ASN.1 encoded OID consists of a sequence of numbers. For convenience, a textual mnemonic shorthand string notation for each OID is used in the text such as "OID". A mapping is given that relates each OID string with the ASN.1 sequence of numbers. Implementations conforming to [ITU-T H.235] shall use only the ASN.1 encoded numbers.

6 System introduction

Figure 2 gives an overview of the scope of this Recommendation within [ITU-T H.323].

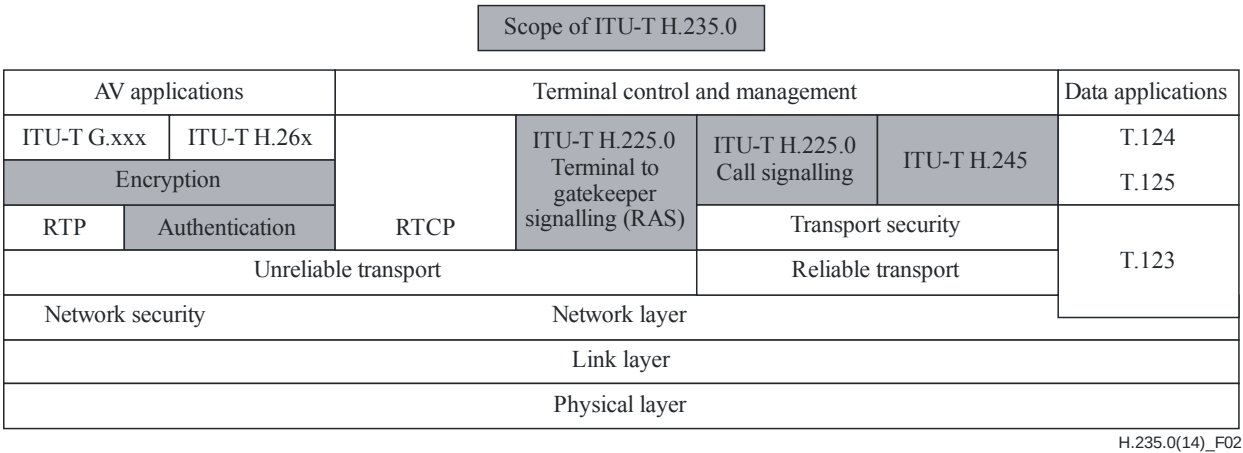


Figure 2 – Overview

For [ITU-T H.323], the signalling of usage of TLS ([IETF RFC 2246], [IETF RFC 3546]), IPsec or a proprietary mechanism on the ITU-T H.245 control channel shall occur on the secured or unsecured ITU-T H.225.0 channel during the initial ITU-T Q.931 message exchange.

6.1 Summary

- 1) The call signalling channel may be secured using TLS ([IETF RFC 2246], [IETF RFC 3546]) or IPsec ([IETF RFC 2401], [b-IETF RFC 2409]) on a secure well-known port ([ITU-T H.225.0]).
- 2) Users may be authenticated either during the initial call connection, in the process of securing the ITU-T H.245 channel and/or by exchanging certificates on the ITU-T H.245 channel.
- 3) The encryption capabilities of a media channel are determined by extensions to the existing capability negotiation mechanism.
- 4) Initial distribution of key material from the master is via ITU-T H.245 **OpenLogicalChannel** or **OpenLogicalChannelAck** messages.
- 5) Re-keying may be accomplished by ITU-T H.245 commands: **EncryptionUpdateCommand**, **EncryptionUpdateRequest**, **EncryptionUpdate** and **EncryptionUpdateAck**.
- 6) Key material distribution is protected either by operating the ITU-T H.245 channel as a private channel or by specifically protecting the key material using the selected exchanged certificates.
- 7) The security protocols presented conform either to ISO published standards or to IETF proposed standards.

6.2 Authentication

The process of authentication verifies that the respondents are in fact who they say they are. Authentication may be accomplished in conjunction with the exchange of public key-based certificates. Authentication may also be accomplished by an exchange which utilizes a shared secret between the entities involved. This may be a static password or some other *a priori* piece of information.

This Recommendation describes the protocol for exchanging the certificates, but does not specify the criteria by which they are mutually verified and accepted. In general, certificates give some assurance to the verifier that the presenter of the certificate is who he says he is. The intent behind the certificate exchange is to authenticate the *user* of the end point, not simply the physical end point. Using digital certificates, an authentication protocol proves that the respondents possess the private keys corresponding to the public keys contained in the certificates. This authentication protects against man-in-the-middle attacks, but does not automatically prove who the respondents are. To do this normally requires that there be some policy regarding the other contents of the certificates. For authorization certificates, for example, the certificate would normally contain the service-provider's identification along with some form of user account identification prescribed by the service provider.

The authentication framework in this Recommendation does not prescribe the contents of certificates (i.e., does not specify a certificate policy) beyond that required by the authentication protocol. However, an application using this framework may impose high-level policy requirements such as presenting the certificate to the user for approval. This higher level policy may either be automated within the application or require human interaction.

For authentication which does not utilize digital certificates, this Recommendation provides the signalling to complete various challenge/response scenarios. This method of authentication requires prior coordination by the communicating entities so that a shared secret may be obtained. An example of this method would be a customer of a subscription-based service.

As a third option, the authentication may be completed within the context of a separate security protocol such as TLS ([IETF RFC 2246], [IETF RFC 3546]) or IKE [b-IETF RFC 2409].

Both bidirectional and unidirectional authentication may be supported by peer entities. This authentication may occur on some or all of the communication channels.

All of the specific authentication mechanisms described in this Recommendation are identical to, or derived from, ISO-developed algorithms as specified in Parts 2 to 3 of [ISO/IEC 9798], or based on IETF protocols.

6.2.1 Certificates

The standardization of certificates, including their generation, administration and distribution is outside the scope of this Recommendation. The certificates used to establish secure channels (call signalling and/or call control) shall conform to those prescribed by whichever protocol has been negotiated to secure the channel.

It should be noted that for authentication utilizing public-key certificates, the end points are required to provide digital signatures using the associated private key value. The exchange of public-key certificates alone does not protect against man-in-the-middle attacks. The ITU-T H.235 protocols conform to this requirement.

6.3 Call establishment security

There are at least two reasons to motivate securing the call establishment channel (e.g., [ITU-T H.323] using [ITU-T Q.931]). The first is for simple authentication, before accepting the call. The second reason is to allow for call authorization. If this functionality is desired in the ITU-T H-series terminal, a secure mode of communication should be used (such as TLS/IPsec for [ITU-T H.323]) before the exchange of call connection messages. Alternatively, the authorization may be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are outside the scope of this Recommendation.

6.4 Call control (ITU-T H.245) security

The call control channel [ITU-T H.245] should also be secured in some manner to provide for subsequent media privacy. The ITU-T H.245 channel shall be secured using any negotiated privacy mechanism (this includes the option of "none"). ITU-T H.245 messages are utilized to signal encryption algorithms and encryption keys used in the shared, private, media channels. The ability to do this on a logical channel by logical channel basis, allows different media channels to be encrypted by different mechanisms. For example, in centralized multipoint conferences, different keys may be used for streams to each end point. This may allow media streams to be made private for each end point in the conference. In order to utilize the ITU-T H.245 messages in a secure manner, the entire ITU-T H.245 channel (logical channel 0) should be opened in a negotiated secure manner.

The mechanism by which the ITU-T H.245 channel is made secure is dependent on the ITU-T H-series terminals involved. The only requirement on all systems that utilize this security structure is that each shall have some manner in which to negotiate and/or signal that the ITU-T H.245 channel is to be operated in a particular secured manner before it is actually initiated. For example, ITU-T H.323 will utilize the ITU-T H.225.0 connection signalling messages to accomplish this.

6.5 Media stream privacy

This Recommendation describes media privacy for media streams carried on packet-based transports. These channels may be unidirectional with respect to ITU-T H.245 logical channel characterizations. The channels are not required to be unidirectional on a physical or transport level.

A first step in attaining media privacy should be the provision of a private control channel on which to establish cryptographic keying material and/or set up the logical channels which will carry the encrypted media streams. For this purpose, when operating in a secure conference, any participating end points may utilize an encrypted ITU-T H.245 channel. In this manner, cryptographic algorithm

selection and encryption keys as passed in the ITU-T H.245 **OpenLogicalChannel** command are protected.

The ITU-T H.245 secure channel may be operated with characteristics different from those in the private media channel(s) as long as it provides a mutually acceptable level of privacy. This allows for the security mechanisms protecting media streams and any control channels to operate in a completely independent manner, providing completely different levels of strength and complexity.

If it is required that the ITU-T H.245 channel be operated in a non-encrypted manner, the specific media encryption keys may be encrypted separately in the manner signalled and agreed to by the participating parties. A logical channel of type **h235Control** may be utilized to provide the material to protect the media encryption keys. This logical channel may be operated in any appropriately negotiated mode.

The privacy (encryption) of data carried in logical channels shall be in the form specified by the **OpenLogicalChannel**. Transport-specific header information shall not be encrypted. The privacy of data is to be based upon end-to-end encryption.

6.6 Trusted elements

The basis for authentication (trust) and privacy is defined by the terminals of the communications channel. For a connection establishment channel, this may be between the caller and a hosting network component. For example, a telephone "trusts" that the network switch will connect it with the telephone whose number has been dialled. For this reason, any entity which terminates an encrypted ITU-T H.245 control channel or any **encryptedData** type logical channel shall be considered a trusted element of the connection; this may include MC(U)s and gateways. The result of trusting an element is the confidence to reveal the privacy mechanism (algorithm and key) to that element.

Given the above, it is incumbent upon participants in the communications path to authenticate any and all "trusted" elements. This will normally be done by certificate exchange as would occur for the "standard" end-to-end authentication. This Recommendation will not require any specific level of authentication, other than to suggest that it be acceptable to all entities using the trusted element. Details of a trust model and certificate policy are for further study.

Privacy can be assured between the two end points only if connections between trusted elements are proven to be protected against man-in-the-middle attacks.

6.6.1 Key escrow

Although not specifically required for operation, this Recommendation contains provision for entities utilizing the ITU-T H.235 protocol to support the facility known as the trusted third party (TTP) within the signalling elements.

The ability to recover lost media encryption keys should be supported in installations where this functionality is desired or required.

Key escrow is a facility which is often referred to as a trusted third party (TTP). This facility is for further study.

6.7 Non-repudiation

For further study.

6.8 Mobility security

ITU-T H.323-based systems may be deployed in a mobility environment according to [ITU-T H.510]. Security procedures and protocols for such systems are described in [ITU-T H.530]. [ITU-T H.530] deploys protocols and procedures from this Recommendation.

6.9 Security profiles

This Recommendation references a couple of security profiles of ITU-T H.235 (i.e., ITU-T H.235.1, ITU-T H.235.2, ITU-T H.235.3, ITU-T H.235.4, ITU-T H.235.5, ITU-T H.235.6, ITU-T H.235.7, ITU-T H.235.8 and ITU-T H.235.9). A security profile specifies specific usage of ITU-T H.235 or a subset of ITU-T H.235 functionality for well-defined environments with scoped applicability.

Depending on the environment and application, security profiles may be implemented either selectively or altogether. Typically, ITU-T H.235-enabled systems indicate within object identifiers as part of signalling messages which security profiles they deploy. ITU-T H.235-enabled systems should choose the security profile according to their needs.

Optionally, end points may initially offer multiple security profiles simultaneously, in **RRQ/GRQ** messages, and let the gatekeeper select the most adequate one by answering it in the **RCF/GCF** message. **LRQ/LCF** transactions between gatekeepers may also carry several security profiles. When calculating digital signatures or hash values to provide message integrity, first the hash values and digital signatures which do not provide message integrity should be calculated over the field subset and set in the message, all the digital signatures and hash values that provide message integrity should be set to zeroes in the message buffer, then all the digital signatures and hash values should be calculated using this buffer, and then set in the message.

Each of the sub-series Recommendations is written as a security profile of ITU-T H.235.0. A security profile of ITU-T H.235.0 typically comprises a use-case specific instantiation of ITU-T H.235.0 within a particular scenario and/or holds a particular security feature specification or a combination of security mechanisms/security profiles.

All security profiles are optional within ITU-T H.235.0.

Figure 3 illustrates some typical and possible combinations of security profiles. A straight line indicates that a pairwise combination of security profiles is defined and possible. A dashed line indicates that a combination is generally possible yet such a combination may not be very useful. Missing lines indicate that a particular combination is not yet defined.

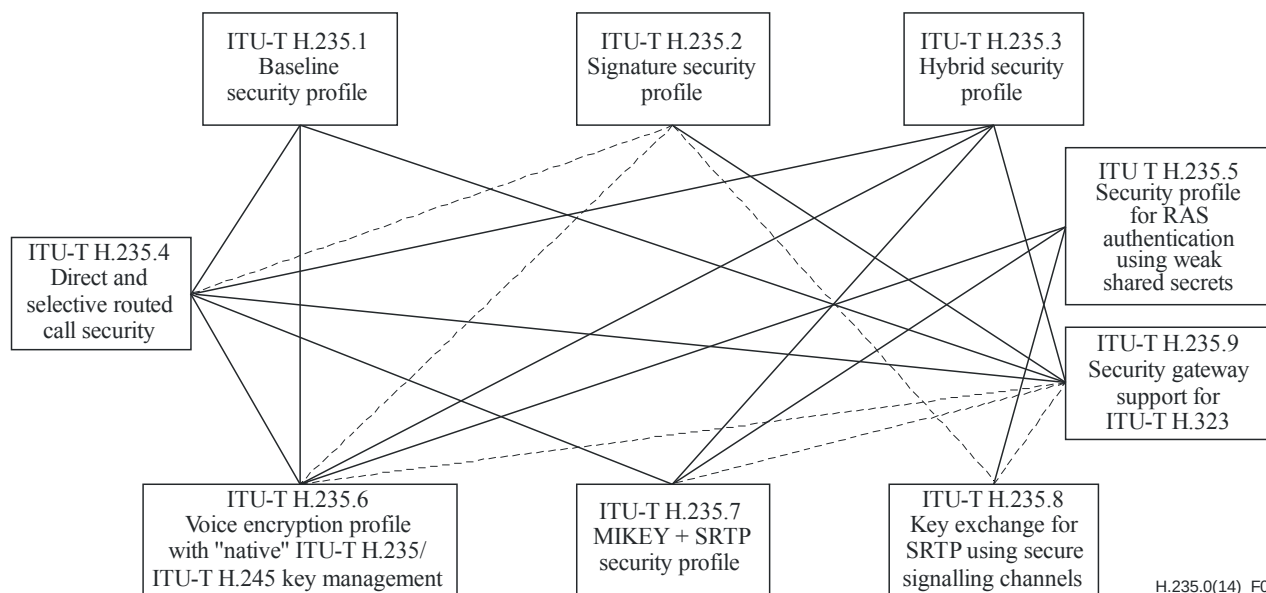


Figure 3 – Illustration of security profile combinations

6.10 Secured NAT/firewall traversal

[ITU-T H.235.9] specifies procedures on how to discover the presence of security gateways (such as ALGs) in the ITU-T H.225.0 RAS signalling path between ITU-T H.323 entities (gatekeeper,