

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.7

(09/2005)

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

H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235

ITU-T Recommendation H.235.7

ITU-T

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.235.7

H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235

Summary

The purpose of this Recommendation is to describe security procedures for H.323/H.235-based systems for using the MIKEY key management protocol in conjunction with the Secure Real Time Transport Protocol.

In earlier versions of the H.235 sub-series, this profile was contained in Annex G/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.235.7 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Media encryption, MIKEY key management, multimedia security, secure Real Time Transport Protocol, security profile, SRTP.

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 and Bibliography	2
3	Definitions	2
4	Symbols and abbreviations	2
5	Conventions	3
6	Introduction	4
7	Overview and scenarios	5
7.1	MIKEY operation at "session level"	6
7.2	MIKEY operation at "media level"	7
7.3	MIKEY capability negotiation	8
8	Security profile using symmetric security techniques.....	9
8.1	Terminating a H.323 call.....	14
8.2	TGK re-keying and CSB updating	15
8.3	H.245 tunnelling support.....	16
8.4	SRTP algorithms	16
8.5	List of object identifiers.....	17
9	Security profile using asymmetric security techniques	17
9.1	Terminating a H.323 call.....	21
9.2	TGK re-keying and CSB updating	21
9.3	H.245 tunnelling support.....	23
9.4	SRTP algorithms	23
9.5	List of object identifiers.....	23
	Appendix I – MIKEY-DHMAC option	23
I.1	Terminating a H.323 call.....	27
I.2	TGK re-keying and CSB updating	28
	Appendix II – Using H.235.4 for establishing a pre-shared secret.....	30
II.1	Terminating a H.323 call.....	32
II.2	TGK re-keying and CSB updating	32

Introduction

The purpose of this Recommendation is to provide recommendations of security procedures for H.323/H.235-based systems to use the IETF MIKEY key management protocol in conjunction with the IETF SRTP security protocol.

This Recommendation is written as a security profile of ITU-T Rec. H.235 that is offered as an option and may complement the other media security features of ITU-T Rec. H.235.6.

This Recommendation enables the deployment of SRTP media security where the MIKEY key management supplies the necessary keys and security parameters among the involved endpoints end-to-end. This Recommendation can be deployed within a H.323 domain among H.235.7-enabled H.323 systems. This Recommendation defines the security protocol extensions to H.225.0 RAS and Call Signalling as well as H.245, along with the corresponding procedures. Furthermore, this Recommendation provides the capabilities to support interworking with IETF SIP entities that have implemented the MIKEY key management and SRTP.

ITU-T Recommendation H.235.7

H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235

1 Scope

The purpose of this Recommendation is to provide recommendations of security procedures for H.323/H.235-based systems to use the MIKEY key management protocol in conjunction with the SRTP security protocol.

This security profile is offered as an option and may complement the other media security features of H.235.6.

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.235.0 (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.235.3 (2005), *H.323 security: Hybrid security profile*.
- ITU-T Recommendation H.235.4 (2005), *H.323 security: Direct and selective routed call security*.
- ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.
- ITU-T Recommendation H.323 (2003), *Packet-based multimedia communication systems*.
- ITU-T Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*.
- ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash functions – Part 3: Dedicated hash functions*.
- IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
- IETF RFC 3711 (2004), *The Secure Real Time Transport Protocol (SRTP)*.
- IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

2.2 Informative references and Bibliography

- IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.
- IETF RFC 2327 (1999), *SDP: Session description protocol*.
- IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method*.
- IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.
- IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.
- IETF RFC ssss (2005), M. Handley, Van Jacobson, C. Perkins: *SDP: Session Description Protocol*, draft-ietf-mmusic-sdp-new-24.txt.
- IETF RFC www (2005), J. Arkko, E. Carrara et al: *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*, Internet Draft draft-ietf-mmusic-kmgmt-ext-14.txt, Work in Progress.
- IETF RFC zzzz (2005), M. Euchner: *HMAC-authenticated Diffie-Hellman for MIKEY*, Internet Draft draft-ietf-msec-MIKEY-DHMAC-11.txt, Work in Progress.

3 Definitions

None.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

a, b, e, d	private DH key of EP A, EP B, GK E, GK D
Cert	digital certificate (see RFC 3830)
CP/C	CallProceeding-to-Connect
CSB	Crypto Session Bundle (see RFC 3830)
CT _B , CT _A	ClearToken for endpoint B, ClearToken for endpoint A (see H.235.4)
DRC1	Direct-routed Call (see H.235.4)
ENC _k (x)	Encryption of X using key k
env_key	Envelope key (RFC 3830) between endpoint B and endpoint A
EP	Endpoint
ESC	H.245 EndSessionCommand
DH	Diffie-Hellman
DH _A	DH half-key of endpoint A
DH _B	DH half-key of endpoint B
g^a, g^b	Diffie-Hellman half-key of EP A, EP B
g^e, g^d	Diffie-Hellman half-key of GK E, GK D
GK	Gatekeeper
HDR	MIKEY header payload (see RFC 3830)
ID _A , ID _B	Identity (i.e., endpoint ID) of endpoint A, Identity of endpoint B

IETF	Internet Engineering Task Force
Imsg	MIKEY message of the initiator (see RFC 3830)
KEMAC	MIKEY KEMAC payload message (see RFC 3830)
$MAC(k, x)$	Keyed MAC on x using key k
Ma	MIKEY authentication key (see RFC 3830)
Me	MIKEY encryption key (see RFC 3830)
MIKEY	Multimedia Internet Keying
NTP	Network Time Protocol
PKE	MIKEY PKE payload message (see RFC 3830)
PKI	Public-Key Infrastructure
PRF	Pseudo-Random Function (MIKEY-PRF, see RFC 3830 sections 4.1.2-4.1.4)
Rand	random nonce (see RFC 3830)
Rmsg	MIKEY message of the responder (see RFC 3830)
rand()	random value
RSA	Rivest, Shamir and Adleman (public key algorithm)
sa, sb	shared secret among endpoint A and GK, shared secret among endpoint B and GK
sl	shared secret among gatekeepers
SDP	Session Description Protocol
SHA1	Secure Hash Algorithm 1 (ISO/IEC 10118-3)
SIP	Session Initiation Protocol
SP	Security Policy (see RFC 3830)
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol (see RFC 3711)
SSRC	Synchronization source (RTP)
T	Timestamp (see RFC 3830)
TGK	Traffic Generating Key (see RFC 3830) between endpoint A and endpoint B
V	Verification message field (see RFC 3830)
ZZ_{AB}	dynamic shared H.323 secret ZZ_{AB}
{ }	Zero, one or more occurrences
[]	Optional element

5 Conventions

The object identifiers are referenced through a symbolic reference in the text (e.g., "G1"), clauses 8.5 and 9.5 list the actual numeric values for the symbolic object identifiers, for further information see also clause 5/H.235.0.

Table 1 defines the five MIKEY key management protocols that are being referenced throughout this Recommendation:

Table 1/H.235.7 – MIKEY key management protocols

MIKEY protocol	Description	OID value	Parameter identifier	Implementation
MIKEY	Any MIKEY protocol	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 76}	76	Mandatory to implement
MIKEY-PS	Symmetric key distribution protocol using pre-shared symmetric keys and HMACs, (see RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 72}	72	Mandatory to implement
MIKEY-DHMAC	Diffie-Hellman key agreement protocol using pre-shared symmetric keys and HMACs; (see RFC zzzz).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 73}	73	Optional
MIKEY-PK-SIGN	(RSA-based) public-key distribution protocol using digital signatures; (see RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 74}	74	Mandatory to implement.
MIKEY-DH-SIGN	Diffie-Hellman key agreement protocol using digital signatures; (see RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 75}	75	Optional

MIKEY (cf. 1st row of Table 1) refers to the MIKEY protocol family generally without indicating specifically any particular MIKEY key management protocol variant such as MIKEY-PS, MIKEY-DHMAC, MIKEY-PK-SIGN or MIKEY-DH-SIGN. The related implementation of MIKEY shall encompass processing of the MIKEY messages such as MIKEY common header payload (RFC 3830 section 6.1), but does not necessarily require any implementation of a particular MIKEY key management protocol or implementation of a particular MIKEY information payload. The corresponding OID and parameter identifier shall be used in those cases where an H.323 endpoint does not know the actually used MIKEY protocol variant. In any other cases, it is recommended to use the specific OID and parameter identifier of the actual MIKEY key management protocol variant instead.

6 Introduction

There has been interest in using the security features of IETF SRTP "Secure Real-time Protocol" from ITU-T Rec. H.235. While former versions of H.235 already offer various media security features such as voice encryption using block ciphers and some limited RTP authentication (anti spam option), there are strong reasons to deploy SRTP:

- use a stream cipher for improved performance, robustness and security;
- be interoperable with other SRTP terminals; such as SIP-based media terminals.

NOTE – This Recommendation does not specify procedures for security interworking with SIP (RFC 3261); this remains for further study;

- yield the improved security for RTCP protection;
- obtain improved integrity spanning the entire RTP/RTCP packet;
- deploy state-of-the art AES encryption algorithm;
- use session encryption/authentication keys derived from a pseudo-random function at both ends.

Further on, a need has been identified to provide an RSA-based key management in addition to the Diffie-Hellman key agreement schemes provided by H.235. Likewise, non-PKI-based key management techniques are felt to be useful in the case where public-key infrastructures are considered not to be the choice. There is also interest to address the issues of lawful interception in the context of key management.

The IETF has also made efforts to define a real-time capable key management scheme MIKEY (RFC 3830). This generic key management scheme interfaces well with SRTP and is able to provide master keys (TGKs) as well as session traffic keys either end-to-end or possibly end-to-middle/hop-by-hop. MIKEY is an optimized key management protocol that completes within at most two messages, making it ideal for fast start call setup in H.323.

This Recommendation provides security procedures to deploy the MIKEY key management protocols from within H.323/H.235 in order to support SRTP media security. It is noted that there might be other alternative ways by which SRTP could be supported within H.323/H.235 but such measures are not addressed in this Recommendation and remain for further study.

This Recommendation deploys the MIKEY key management protocols in a manner that is conceptually similar to the approach described in RFC www where SIP (RFC 3261) carries MIKEY within SDP (RFC 2327, RFC ssss and RFC 3264).

This Recommendation provides two security profiles with security procedures for two very distinct security infrastructures:

- symmetric key-based security infrastructure supporting multiple gatekeepers (see clause 8); and
- asymmetric key-based security infrastructure (PKI) supporting multiple gatekeepers (see clause 9).

7 Overview and scenarios

Figure 1 shows the general scenario that this Recommendation addresses. At least two distinct H.323 endpoints A and B are part of this scenario. These endpoints may be H.323 terminals or H.323 media gateways, the latter with potential interface to other packet- or non-packet-based networks. In addition, at least one gatekeeper is assumed to be part of the environment. In case, there is only a single gatekeeper available, it is assumed that all H.323 endpoints are within that single gatekeeper zone only. In case multiple, chained gatekeepers exist, H.323 endpoints may be placed within different gatekeeper zones. It is further assumed that H.323 endpoints communicate directly end-to-end using the RTP media protocol.

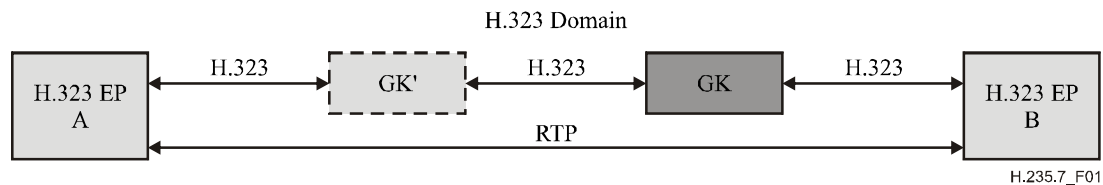


Figure 1/H.235.7 – Scenario

Figure 2 shows the general security scenario indicating the usage of the MIKEY key management protocols and the SRTP media security protocol. The MIKEY key management protocols run between the H.323 endpoints A and B; the MIKEY key management protocols are encapsulated within containers within the H.245 signalling handshakes (Terminal Capability Set, Request Mode, Open Logical Channel handshakes and MiscellaneousCommand) and are transparent to any intermediate Gatekeeper(s).

It is noted that an H.323 endpoint may actually be a gateway. For example, such a gateway may provide an interworking function to interface with SIP-based systems. In this case, the gateway may not necessarily terminate MIKEY but may further relay MIKEY and extend MIKEY for truly end-to-end key management among the involved multimedia terminals, thereby supporting end-to-end media security with SRTP. This approach would support security interworking between H.323/H.235 and SIP-based systems. The exact interworking functionality or specification of such gateways is not the subject of this Recommendation and remains for further study.

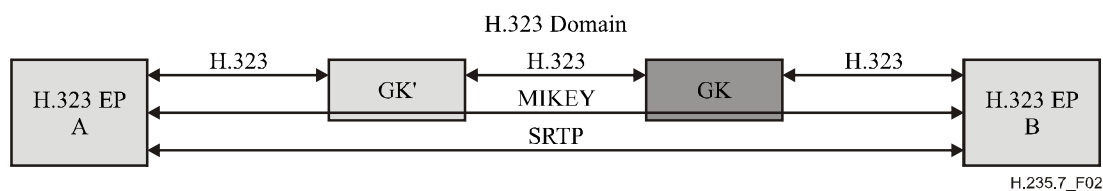


Figure 2/H.235.7 – Security scenario with MIKEY and SRTP

All the key management protocols described in this Recommendation proceed in two stages:

- Stage 1 occurs during the H.225.0 RAS and Call Signalling phase. For the symmetric-key MIKEY protocols (MIKEY-PS or MIKEY-DHMAC) this stage establishes an end-to-end shared ZZ_{AB} between the endpoints A and B that is deployed as a pre-shared secret for MIKEY. For the asymmetric MIKEY protocols (MIKEY-PK-SIGN and MIKEY-DH-SIGN) this stage establishes dynamic shared secrets between the endpoint and its next hop (typically its serving gatekeeper); the dynamic shared secret is not related to MIKEY but serves to secure the H.225.0 Call Signalling between the endpoint and its next hop.
- Stage 2 occurs during the H.225.0 Call Signalling/H.245 protocol phases. This stage negotiates and runs the MIKEY protocol (MIKEY-PS, MIKEY-DHMAC, MIKEY-PK-SIGN or MIKEY-DH-SIGN) between the endpoints A and B and establishes the MIKEY TGK. During stage 2, the MIKEY endpoints may also run the MIKEY re-keying and key update protocol to refresh or update the TGK. Terminating a call and discarding key material (TGK) may further occur during stage 2.

7.1 MIKEY operation at "session level"

The MIKEY key management protocols may operate on a "session-level"; i.e., the MIKEY TGK is applied for more than one media stream. It is recommended to run MIKEY at "session level" during the **TerminalCapability** handshake.