

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.8

(09/2005)

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

H.323 security: Key exchange for SRTP using secure signalling channels

ITU-T Recommendation H.235.8



International
Telecommunication
Union

Documents
Document Sharing Hub

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.235.8

H.323 security: Key exchange for SRTP using secure signalling channels

Summary

The purpose of this Recommendation is to describe security procedures for key exchange for SRTP using secure signalling channels over H.323/H.235 networks.

This Recommendation should be used in conjunction with ITU-T Recs H.323 and H.225.0 versions 4 or later.

Source

This Recommendation H.235.8 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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.....	2
2.1	Normative references.....	2
2.2	Informative references.....	2
3	Symbols and abbreviations	2
4	Parameter description	3
4.1	SRTP parameter transport	3
4.2	SrtpCryptoCapability parameter description.....	4
4.3	SrtpKeys parameter description	6
4.4	SRTP crypto context initialization	7
5	Procedures	9
5.1	Security capability exchange.....	9
5.2	Initial negotiation.....	10
5.3	Session modification	13
5.4	No negotiation	14
5.5	Forward error correction.....	14
6	Public key cryptography to secure key exchange for SRTP	14
6.1	Endpoint identification	15
6.2	SRTP key exchange procedures	15
6.3	CMS body usage.....	16
7	H.235 SRTP security descriptions syntax	19

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

ITU-T Recommendation H.235.8

H.323 security: Key exchange for SRTP using secure signalling channels

1 Scope

The purpose of this Recommendation is to provide recommendations for security procedures to support the IETF Secure Real Time Protocol (SRTP) between H.323 Endpoints in cases where the cryptographic material for the media channel is transported over a secure signalling channel, e.g., IPsec (RFC 2401), TLS (RFC 2246) or other H.235 mechanisms. These security procedures are offered as an alternative to other H.235 security procedures that support SRTP.

This Recommendation describes procedures used to support the IETF Secure Real Time Protocol (SRTP) in ITU-T Rec. H.323. SRTP provides security services for RTP media and relies on separate protocols to provide key management services and the negotiation of cryptographic parameters. These procedures should not be used when the secure signalling channel terminates at an intermediate system, in such cases the SRTP cryptographic material should be transported by a secure end-to-end mechanism.

These procedures support the signalling, negotiation and transport of the SRTP cryptographic keys, authentication and encryption algorithm identifiers and other session parameters between H.323 Endpoints.

A key aspect of these procedures is that the H.245 slave as well as the H.245 master shall be able to generate and distribute cryptographic keys.

SRTP security capabilities may be exchanged using existing terminal capabilities exchange using h235SecurityCapability entries in the capabilityTable of the H.245 TerminalCapabilitySet message. The genericH235SecurityCapability field in the encryptionAuthenticationAndIntegrity field in the h235SecurityCapability entry contains the SrtCryptoCapability field which will specify the SRTP crypto-suites.

A SRTP crypto parameter is specified to signal and negotiate SRTP cryptographic parameters. The definition of the crypto parameter in this Recommendation is limited to two-party unicast media streams where each source has a unique cryptographic key; support for multicast media streams or multipoint unicast streams is for further study.

The SRTP crypto parameter is intended to be able to establish the SRTP cryptographic parameters in a single message or a single round trip message exchange. In the case of a round trip message exchange, the cryptographic parameters may be negotiated. For example, in Fast Connect, the offering H.323 Endpoint sends a set of offered SRTP crypto parameters to the answering H.323 Endpoint, each offer encapsulated in a separate H.245 OpenLogicalChannel message. The answering H.323 Endpoint may then accept one of the offered parameters and respond with an answer that includes the selected parameter subset encapsulated in a H.245 OpenLogicalChannel message.

In the case of a single message exchange there is no negotiation. The offering H.323 Endpoint sends the SRTP crypto parameters to the answering H.323 Endpoint which either accepts the offered parameters or rejects the call.

Public key cryptography procedures may be added to provide end-to-end confidentiality and authentication of the SRTP session key material exchanged between H.323 Endpoints by encrypting and then signing the SRTP key material in the case where the encapsulating security protocol, e.g., IPsec, TLS, terminates on an intermediate device and, therefore, does not provide end-to-end security.

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.323 (2003), *Packet-based multimedia communications systems*.
- ITU-T Recommendation H.460.11 (2004), *Delayed call establishment within H.323 Systems*.
- IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.
- IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.
- IETF RFC 2733 (1999), *An RTP Payload Format for Generic Forward Error Correction*.
- IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- 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 3852 (2004), *Cryptographic Message Syntax (CMS)*.

2.2 Informative references

- IETF Draft, F. Andreasen, M. Baugher, D. Wing: *Session Description Protocol Security Descriptions for Media Streams*, <draft-ietf-mmusic-sdescriptions-11.txt>.

3 Symbols and abbreviations

This Recommendation uses the following abbreviations:

AES	Advanced Encryption Algorithm
ASN.1	Abstract Syntax Notation One
CA	Certificate Authority
CEK	Content Encryption Key
CMS	Cryptographic Message Syntax
EP	Endpoint
FEC	Forward Error Correction
FFS	For Further Study
F8	UMTS Encryption Algorithm
GK	Gatekeeper

GW	Gateway
HMAC	Keyed-Hash Message Authentication Code
IETF	Internet Engineering Task Force
KDR	Key Derivation Rate
MAC	Message Authentication Code
MKI	Master Key Identifier
OID	Object Identifier
OLC	Open Logical Channel
PKI	Public Key Infrastructure
RAS	Registration, Admission, Status
ROC	Roll-over Counter
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SHA1	Secure Hash Algorithm 1
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
SSRC	Synchronization Source
TLS	Transport Level Security
WSH	Window Size Hint

4 Parameter description

SRTP cryptographic capability and key material is exchanged using two parameters:

- **SrtpCryptoInfo** within **SrtpCryptoCapability** shall contain the crypto-suite and session parameters. The **SrtpCryptoInfo** parameter shall be transported in the H.245 **genericH235SecurityCapability** parameter to signal and negotiate SRTP cryptographic parameters.
- **SrtpKeyParameters** within **SrtpKeys** shall contain the SRTP key material. The **SrtpKeys** container in the H.245 **h235Key** parameter shall transport one or more **SrtpKeyParameters** with the SRTP keys.

The use of the SRTP crypto parameters in this Recommendation is limited to two-party unicast media streams where each source has a unique cryptographic key; support for multicast media streams or multipoint unicast streams is for further study.

4.1 SRTP parameter transport

A full-duplex SRTP media connection consists of two unidirectional channels, one in each direction. Each crypto-offer is transported in a separate H.245 **OpenLogicalChannel** message.

4.1.1 SrtpKeys transport

The SRTP cryptographic key material **SrtpKeys** shall be transported in the **genericKeyMaterial** field of the **secureSharedSecret (V3KeySyncMaterial)** parameter contained within the **h235Key** container in the **encryptionSync** parameter of H.245 **OpenLogicalChannel** messages.

The SRTP cryptographic key content in the **genericKeyMaterial** container shall be identified using the H.235.8 object identifier value (see Table 1) in the **standard** field of **capabilityIdentifier**

