

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.248.77

(12/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication
procedures

Gateway control protocol: Secure real-time transport protocol (SRTP) package and procedures

Recommendation ITU-T H.248.77

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
Telepresence	H.420–H.429
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
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	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	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
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.248.77

Gateway control protocol: Secure real-time transport protocol (SRTP) package and procedures

Summary

Recommendation ITU-T H.248.77 defines a new ITU-T H.248 package, the secure real-time transport protocol (SRTP) package. In addition, this Recommendation covers a set of procedures related to SRTP key management. The combination of package and procedures allows a media gateway controller (MGC) to control the use of SRTP by a media gateway (MG).

This revision contains an updated package that allows for the usage of datagram transport layer security (DTLS)-SRTP key management scheme that exchanges the peers' certificates via the signalling path and then establishes a DTLS connection on the bearer path.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.248.77	2010-09-13	16	11.1002/1000/10987
2.0	ITU-T H.248.77	2017-12-14	16	11.1002/1000/13432

Keywords

Key management, SRTP.

* 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 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 2018

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 Connection model.....	1
2	References.....	2
3	Definitions	3
	3.1 Terms defined elsewhere	3
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Secure RTP package	4
	6.1 Properties.....	4
	6.2 Events	6
	6.3 Signals	7
	6.4 Statistics.....	7
	6.5 Error codes.....	9
	6.6 Procedures	9
7	Key management using SDP security descriptions	11
	7.1 Overspecification of SRTP parameters and multiple keys.....	12
	7.2 Wildcarding of SRTP parameters.....	12
	7.3 Interoperability with offer/answer-based implementations.....	13
	7.4 SDES and SRTP cryptographic contexts	13
	7.5 Mapping of master keys for sent packets and received packets statistics	14
8	Key management using DTLS-SRTP	14
	8.1 Key management indication	15
	8.2 Bearer plane connection for "DTLS-SRTP"	15
	8.3 Multi key management operation	17
9	Security considerations	17
	9.1 Relation to key management scheme "SDES"	17
	9.2 Relation to key management scheme "DTLS-SRTP"	17
	Appendix I – Example call flows for key management scheme "SDES"	18
	I.1 Initial session setup using SDP security descriptions.....	18
	I.2 MG1's key is about to expire	21
	I.3 Auditing SRTP capabilities	21
	I.4 Auditing of SRTP statistics	22
	Appendix II – Sample use-cases of SRTP bearer encryption	24
	II.1 Use-case #1: ITU-T H.248 MG for peering IP and circuit-switched networks	24
	II.2 Use-case #2: ITU-T H.248 MG for peering IP networks	24
	II.3 Use-case #3: Transparent SRTP forwarding	25
	Bibliography.....	27

Recommendation ITU-T H.248.77

Gateway control protocol: Secure real-time transport protocol (SRTP) package and procedures

1 Scope

The secure real-time transport protocol (SRTP) is a real-time transport protocol (RTP) profile that provides confidentiality, message authentication and replay protection to RTP and RTP control protocol (RTCP) sessions. The secure RTP package allows a media gateway controller (MGC) to control the use of SRTP by a media gateway (MG). This package is defined in detail in clause 6.

By itself, the secure RTP package is incomplete, as it does not provide procedures for key management. Instead, it is designed to rely on existing key-management schemes (see also [b-IETF RFC 7202]). [b-IETF RFC 5479] provides an example selection of key-management protocol options for SRTP in "SIP networks".

Clause 7 provides procedures for the use of one such key-management scheme: session description protocol (SDP) security descriptions.

Clause 8 provides procedures for the use of one such key-management scheme: datagram transport layer security (DTLS)-SRTP.

Several reasons exist why this Recommendation is required, in addition to the existing (usually SDP-based) SRTP key-management schemes. The most significant of which are listed below:

- Most existing SDP key-management schemes rely on the SDP offer/answer model (see [b-IETF RFC 3264]). However, the offer/answer model is not used in ITU-T H.248 as it does not fit the nature of the connection between an ITU-T H.248 MGC and a MG.
- Existing SDP key-management schemes do not contain procedures relating to parameter overspecification and wildcarding, which are unique to ITU-T H.248.
- The limited lifetime of SRTP master keys calls for mechanisms for handling master key expiry. The existing mechanisms cannot be used in ITU-T H.248.
- The SRTP package allows explicit control over the key-management scheme employed, allowing easy interoperability with, and migration to future schemes.
- The SRTP package allows an MGC to audit the SRTP capabilities of an MG through the use of the packages descriptor and the properties of the new package.
- The SRTP package allows an MGC to collect statistics regarding the number of security violations encountered by the MG, and the volume of SRTP traffic it processed.

The scope of the (09/2010) edition of this Recommendation is limited to use-cases in which a MG applies SRTP procedures, as described in section 3.3 of [IETF RFC 3711], to the SRTP packets it sends and receives. Use-cases in which the MG handles SRTP packets without using those procedures (e.g., transparent forwarding, storage in encrypted form, etc.) are intentionally left out of this Recommendation.

This revision (12/2017) of the Recommendation extends the scope for further SRTP key management schemes, such as DTLS-SRTP according to [b-IETF RFC 5763] and [IETF RFC 5764].

1.1 Connection model

All protocol elements and procedures described in this Recommendation are limited to the extent of a single ITU-T H.248 termination. In addition, no assumptions are made regarding either the lower layer protocols beneath the SRTP level or the upper layer protocols/codecs being carried by the SRTP.

Document Sharing Hub

This allows the use of the Recommendation's procedures in various connection models and use-cases (e.g., an SRTP-enabled announcement server, an SRTP to RTP translator, etc.).

Figure 1 details the generic connection-model where an SRTP-enabled termination is connected to a single other termination (either SRTP-enabled or not). The generalization to any number of terminations is trivial.

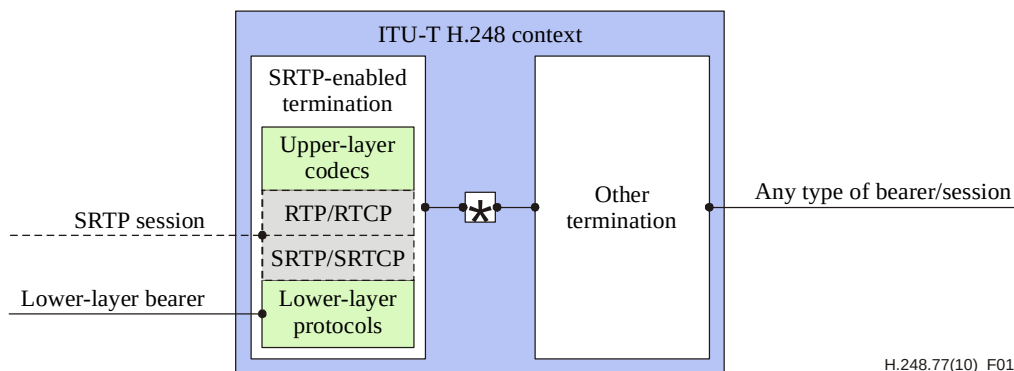


Figure 1 – Two-termination context with an SRTP termination

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.248.1] Recommendation ITU-T H.248.1 (2013), *Gateway control protocol: Version 3*.
- [ITU-T H.248.8] Recommendation ITU-T H.248.8 (2013), *Gateway control protocol: Error code and service change reason description*.
- [ITU-T H.248.47] Recommendation ITU-T H.248.47 (2008), *Gateway control protocol: Statistic conditional reporting package*.
- [ITU-T H.248.49] Recommendation ITU-T H.248.49 (2007), *Gateway control protocol: Session description protocol RFC and capabilities packages*.
- [ITU-T H.248.90] Recommendation ITU-T H.248.90 (2014), *Gateway control protocol: ITU-T H.248 packages for control of transport security using transport layer security (TLS)*.
- [ITU-T H.248.93] Recommendation ITU-T H.248.93 (2014), *Gateway control protocol: ITU-T H.248 support for control of transport security using the datagram transport layer security (DTLS) protocol*.
- [IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
- [IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.
- [IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams*.

- [IETF RFC 4572] IETF RFC 4572 (2017), *Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)*.
- [IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.
- [IETF RFC 5764] IETF RFC 5764 (2010), *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*.
- [IETF RFC 6347] IETF RFC 6347 (2012), *Datagram Transport Layer Security Version 1.2*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 RTP session (section 2.2.2 of [b-IETF RFC 7656] | [b-ITU-T H.248.95]): An association among a group of participants communicating with RTP. It is a group communications channel which can potentially carry a number of RTP Streams. Within an RTP Session, every Participant can find meta-data and control information (over RTCP) about all the RTP Streams in the RTP Session. The bandwidth of the RTCP control channel is shared between all Participants within an RTP Session.

3.1.2 SRTP cryptographic context [IETF RFC 3711]: The set of cryptographic state information that an SRTP sender or receiver must maintain per SRTP session participant.

NOTE – This term is often abbreviated as "crypto context".

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 decrypting master key: An SRTP master key used to decrypt and authenticate SRTP packets received by the MG.

3.2.2 encrypting master key: An SRTP master key used to encrypt and authenticate SRTP packets sent by the MG.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
DTLS	Datagram Transport Layer Security
HMAC	Keyed-Hash Message Authentication Code
IP	Internet Protocol
IPSec	IP Security
ISDN	Integrated Services Digital Network
L1	Layer 1 (of the Open Systems Interconnection model – the physical layer)
L2	Layer 2 (of the Open Systems Interconnection model – the data link layer)
MG	Media Gateway
MGC	Media Gateway Controller
MKI	Master Key Identifier

NAPT	Network Address and Port Translation
NAT	Network Address Translation
PSTN	Public Switched Telephone Network
ROC	Rollover Counter
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SAVP	Secure Audio-Video Profile
SDES	Session Description Protocol Security Descriptions
SDP	Session Description Protocol
SHA1	Secure Hash Algorithm 1
SRTCP	Secure RTCP
SRTP	Secure RTP
SSRC	Synchronization Source
TDM	Time Division Multiplexing
TLS	Transport Layer Security
UDP	User Datagram Protocol
WebRTC	Web Real-Time Communications

5 Conventions

The names of ITU-T H.248 descriptors are always capitalized, for example, Streams and Local Descriptor.

The names of ITU-T H.248 properties, events, signals and parameters appear in the text in italics, for example *ReserveValue*.

All error codes appearing in this Recommendation are described in [ITU-T H.248.8] and [ITU-T H.248.49].

6 Secure RTP package

Package name:	Secure RTP
Package ID:	srtcp (0x0107)
Description:	This package defines elements that allow the MGC to control an MG's use of the SRTP profile. Version 2 adds support for key management via DTLS for SRTP [IETF RFC 5764].
Version:	2
Extends:	None

6.1 Properties

6.1.1 Supported Encryption Transforms

Property name:	Supported Encryption Transforms
Property ID:	set (0x0001)

Description:	This property declares the set of encryption transforms that can be used by SRTP sessions.
Type:	Sub-list of Enumeration
Possible values:	Each item in the list can be one of: "NULL" (0x0000): The NULL Cipher "AES_CM_128" (0x0001): AES in counter mode with a 128-bit key "AES_CM_192" (0x0002): AES in counter mode with a 192-bit key "AES_CM_256" (0x0003): AES in counter mode with a 256-bit key "AES_F8_128" (0x0004): AES in f8 mode with a 128-bit key "AES_F8_192" (0x0005): AES in f8 mode with a 192-bit key "AES_F8_256" (0x0006): AES in f8 mode with a 256-bit key
Default:	Provisioned
Defined in:	TerminationState
Characteristics:	ReadOnly

6.1.2 Supported Authentication Transforms

Property name:	Supported Authentication Transforms
Property ID:	sat (0x0002)
Description:	This property declares the set of authentication transforms that can be used by SRTP sessions.
Type:	Sub-list of Enumeration
Possible values:	Each item in the list can be one of: "NULL" (0x0000): The NULL authentication algorithm "HMAC_SHA1_80" (0x0001): HMAC-SHA1 with an 80-bit tag "HMAC_SHA1_32" (0x0002): HMAC-SHA1 with a 32-bit tag
Default:	Provisioned
Defined in:	TerminationState
Characteristics:	ReadOnly

6.1.3 Key Management Scheme

Property name:	Key Management Scheme
Property ID:	km (0x0003)
Description:	This property controls the key management scheme that will be used for supplying the SRTP parameters and keys
Type:	Enumeration
Possible values:	"None" (0x0000): No key management will be used. "SDS" (0x0001): SDP security descriptions [IETF RFC 4568] "DTLS-SRTP" (0x0002): DTLS-SRTP [IETF RFC 5764]
Default:	"None", unless provisioned otherwise
Defined in:	TerminationState
Characteristics:	Read/Write