International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.77

(09/2010)

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 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
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

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 RTP package. In addition, this Recommendation covers a set of procedures related to SRTP key management. The combination of package and procedures allows a MGC to control the use of secure RTP (SRTP) by a MG.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.248.77	2010-09-13	16

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/.

CONTENTS

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 an RTP profile that provides confidentiality, message authentication and replay protection to RTP and RTCP sessions. The secure RTP package allows a MGC to control the use of SRTP by a 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. Clause 7 provides procedures for the use of one such key-management scheme: SDP security descriptions.

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 this Recommendation is limited to use-cases in which a MG applies SRTP procedures, as described in clause 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.

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

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

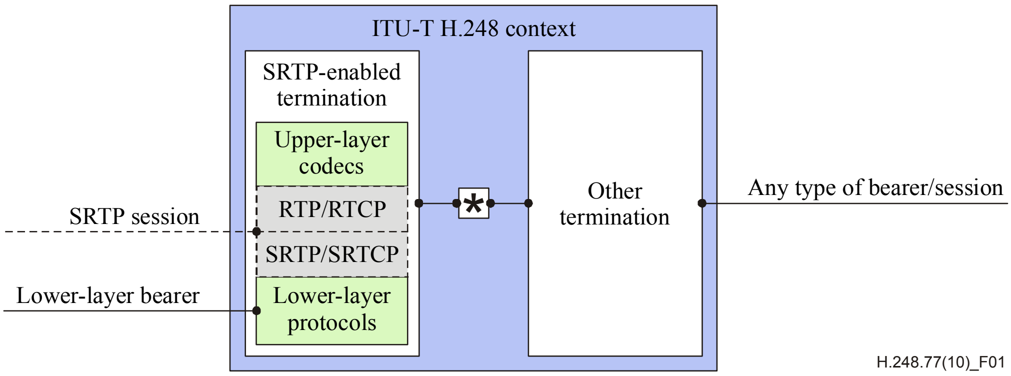


Figure 1 – Two-termination context with a SRTP termination

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 (2005), *Gateway control protocol: Version 3,* including its Amendment 1 (2008) and Amendment 2 (2009).

[ITU-T H.248.8] Recommendation ITU-T H.248.8 (2007), *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*.

[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*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 RTP session [IETF RFC 3550]: An association among a set of participants communicating with RTP. The distinguishing feature of an RTP session is that each maintains a full, separate space of SSRC identifiers.

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 1 – 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: A SRTP master key used to decrypt and authenticate SRTP packets received by the MG.

3.2.2 encrypting master key: A 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
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
SDP	Session Description Protocol
SHA1	Secure Hash Algorithm 1
SRTCP	Secure RTCP
SRTP	Secure RTP
SSRC	Synchronization Source
TDM	Time Division Multiplexing
UDP	User Datagram Protocol

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:	srtp (0x0107)
Description:	This package defines elements that allow the MGC to control an MG's use of the SRTP profile.
Version:	1
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.

"SDES" (0x0001): SDP security descriptions [IETF RFC 4568]

Default: "None", unless provisioned otherwise

Defined in: TerminationState

Characteristics: Read/Write

6.1.4 Key Lifetime Expiry Behaviour

Property Name: Key Lifetime Expiry Behaviour

Property ID: kleb (0x0004)

Description: This property indicates which actions should be taken upon the expiry of the encrypting master key. The MG triggers key lifetime expiry when it determines that it has used the SRTP master key for the maximal number of packets allowed (by default 2^{48} SRTP and/or 2^{31} SRTCP packets; this value can be lowered through key-management).

See clause 6.6.3 and clause 9.2 of [IETF RFC 3711] for further information regarding master key lifetime expiry.

Type: Enumeration

Possible values: "DROP" (0x0000): Do not close SRTP session, drop all packets

"BYE" (0x0001): Close SRTP session, send SRTCP BYE

Default: "DROP", unless provisioned otherwise

Defined in: LocalControl

Characteristics: Read/Write

6.2 Events

6.2.1 Master Key Expiry

Event Name: Master Key Expiry

Event ID: mke (0x0001)

Description: This event allows the MGC to be notified when the encrypting SRTP master key is about to expire (watermark threshold crossed) or has already expired. As the lifetime is media-stream specific, when multiple streams are defined on a termination, this event shall be notified on a specific stream only.

NOTE – If the watermarks are set to 0, notification will be sent only upon master key expiration.

6.2.1.1 EventsDescriptor Parameters

6.2.1.1.1 SRTP Watermark

Parameter Name: SRTP Watermark

Parameter ID: rtpw (0x0001)

Description: The number of SRTP packets that the master key can still support when the event is first notified.

Type: Double (Note)

Optional: Yes

Possible Values: Any non-negative value.

Default: 0, unless provisioned otherwise

NOTE – The maximal master key lifetime is 2^{48} SRTP packets and 2^{31} SRTCP packets. Therefore, the SRTP Watermark and SRTCP Watermark parameters are of type Double and Unsigned Integer, respectively.

6.2.1.1.2 SRTCP Watermark

Parameter Name: SRTCP Watermark

Parameter ID: rtcpw (0x0002)

Description: The number of SRTCP packets that the master key can still support when the event is first notified.

Type: Unsigned Integer (Note)

Optional: Yes

Possible Values: Any non-negative value.

Default: 0, unless provisioned otherwise

NOTE – The maximal master key lifetime is 2^{48} SRTP packets and 2^{31} SRTCP packets. Therefore, the SRTP Watermark and SRTCP Watermark parameters are of type Double and Unsigned Integer, respectively.

6.2.1.2 ObservedEventsDescriptor Parameters

6.2.1.2.1 Key Expired

Parameter Name: Key Expired

Parameter ID: ke (0x0001)

Description: The parameter indicates whether, at the time of notification, the master key is still valid or has already expired.

Type: Boolean

Optional: Yes

Possible Values: True: The number of SRTP and SRTCP packets has met the master key lifetime, i.e., the key has already expired.

False: The number of SRTP and SRTCP packets is still within the master key's lifetime.

Default: False

6.3 Signals

None.

6.4 Statistics

6.4.1 Number of Replayed Packets

Statistic Name: Number of Replayed Packets

Statistic ID: replay (0x0001)

Description: This statistic logs the number of received packets that have been judged to be replayed and discarded, according to clause 3.3 of [IETF RFC 3711], since the instantiation of the statistic.

Type: Double

Possible values: Any non-negative value

Level: Either

6.4.2 Number of Authentication Failures

Statistic Name: Number of Authentication Failures

Statistic ID: authfail (0x0002)

Description: This statistic logs the number of packets that have failed authentication and been discarded, according to clause 3.3 of [IETF RFC 3711], since the instantiation of the statistic.

Type: Double

Possible values: Any non-negative value

Level: Either

6.4.3 Sent SRTP Packets Protected by Master Key

Statistic Name: Sent SRTP Packets Protected by Master Key

Statistic ID: srpk (0x0003)

Description: This statistic logs the number of sent SRTP packets that were protected by each of the current master key(s).

Type: Sub-list of Double. Each element in the list corresponds to one of the encrypting master keys. The mapping between keys and list positions depends on the key management scheme employed.

Possible values: Any non-negative value

Level: Stream

6.4.4 Sent SRTCP Packets Protected by Master Key

Statistic Name: Sent SRTCP Packets Protected by Master Key

Statistic ID: scpk (0x0004)

Description: This statistic logs the number of sent SRTCP packets that were protected by each of the current master key(s).

Type: Sub-list of Unsigned Integer. Each element in the list corresponds to one of the encrypting master keys. The mapping between keys and list positions depends on the key management scheme employed.

Possible values: Any non-negative value

Level: Stream

6.4.5 Received SRTP Packets Protected by Master Key

Statistic Name: Received SRTP Packets Protected by Master Key

Statistic ID: rrpk (0x0005)

Description: This statistic logs the number of received SRTP packets that were protected by each of the current master key(s).

Type: Sub-list of Double. Each element in the list corresponds to one of the decrypting master keys. The mapping between keys and list positions depends on the key management scheme employed.

Possible values: Any non-negative value

Level: Stream

6.4.6 Received SRTCP Packets Protected by Master Key

Statistic Name: Received SRTCP Packets Protected by Master Key

Statistic ID: rcpk (0x0006)

Description: This statistic logs the number of received SRTCP packets that were protected by each of the current master key(s).

Type: Sub-list of Unsigned Integer. Each element in the list corresponds to one of the decrypting master keys. The mapping between keys and list positions depends on the key management scheme employed.

Possible values: Any non-negative value

Level: Stream

6.5 Error codes

None.

6.6 Procedures

6.6.1 Determining cryptographic capabilities

The MGC can determine the cryptographic transforms that an MG supports by auditing the value of the *Supported Encryption Transforms* (*set*) and *Supported Authentication Transforms* (*sat*) properties. Usually, these properties are only available on the Root termination, and convey the cryptographic capabilities of the MG as a whole. However, it is possible that some use-cases will call for the support of these properties on non-Root terminations. One example would be a case where different terminations have different cryptographic capabilities.

The *Supported Encryption Transforms* and *Supported Authentication Transforms* properties declare a value for the NULL cipher and the NULL authentication algorithm respectively. By including these values, a MG explicitly indicates that its policy allows the use of unencrypted and/or unauthenticated SRTP and SRTCP packets. Note that, in accordance with [IETF RFC 3711], SRTCP packets must be authenticated using a non-NULL algorithm, regardless of the declared support of the NULL authentication algorithm.

6.6.2 Key management

The SRTP package does not define protocol elements for performing SRTP key management. Instead, the *Key Management Scheme* (*km*) property allows the MGC to indicate the use of one of several, already established, key management schemes.

The only key management scheme supported by version 1 of the package is the use of SDP security descriptions (see [IETF RFC 4568]) in the Local and Remote Descriptors. Further details about the adaptation of these security descriptions for use in ITU-T H.248 are provided in clause 7. Future versions of this package may allow the use of additional key management schemes, for example, SDP key management extensions (see [b-IETF RFC 4567]).

By default, the value of the *Key Management Scheme* property is "None"; indicating that no key management is used, and therefore SRTP is not employed. This prevents an MGC that is unaware of this package from inadvertently "turning on" SRTP through the careless inclusion of SDP parameters in the Local and Remote Descriptors.

6.6.3 Master key lifetime

SRTP master keys have a limited lifetime, measured in the number of SRTP and SRTCP packets that may be protected using the same key. The *Master Key Expiry* (*mke*) event allows the MGC to be notified when the master key is close to being, or has already been exhausted. The MG notifies this event based on the expiry status of the key used to encrypt and authenticate sent packets. No notification is generated regarding the expiry of the decrypting master key used for handling received packets.

The *SRTP Watermark* (*rtpw*) and *SRTCP Watermark* (*rtcpw*) event parameters allow the MGC to control how long before key exhaustion the *mke* event is first notified. If the value of the relevant watermark is different from 0, the MG shall generate the event when the master key has been used for (lifetime – *rtpw*) SRTP packets or (lifetime – *rtcpw*) SRTCP packets (whichever happens first). For example, if the key lifetime is 2^{20}, and *rtpw* and *rtcpw* are both equal to 2^{16}, the event will be notified after (2^{20}–2^{16} = 983040) SRTP or SRTCP packets have been protected by that key.

Regardless of the value of the *rtpw* and *rtcpw* parameters, the *Master Key Expiry* event shall be notified by the MG when the master key has fully expired and can no longer be used. The MGC can differentiate whether the master key has already expired or only the SRTP/SRTCP watermark was crossed through the *Key Expired* parameter.

When several master keys can be used by the MG, the gateway shall generate the *mke* event only when all master keys are about to be, and/or have already been exhausted. For example, if three keys are used in series, each with a lifetime of *X* packets, the MG shall first send a notification only after the third (and last) key has been used for *X-rtpw* SRTP packets or *X-rtcpw* SRTCP packets. An additional notification will be sent when the third key has been fully exhausted.

The *mke* event may be configured on a specific stream or on the complete termination. Configuring the *mke* event on a termination is equivalent to configuring it, with the same parameter values, on each of these termination's streams (other than streams that already have the event explicitly enabled). As different streams may exhaust the key at different times, an *mke* notification shall always be associated with a specific Stream.

6.6.3.1 MG behaviour at key exhaustion

The operations taken by the MG when the last encrypting master key is exhausted are controlled through the *Key Lifetime Expiry Behaviour* (*kleb*) property. Setting this property to "BYE" will cause the MG to send an SRTCP BYE packet, hence leaving the RTP session or closing it (if it is the session's sole sender) as soon as the master-key expires.

NOTE – The MG must ensure that it is able to send the SRTCP BYE packet using a valid master key. This means that when *kleb* is set to "BYE", the encrypting master key will expire when it can still protect one additional SRTCP packet.

If the MGC installs a new master key after the MG has sent an SRTCP BYE packet, the MG will rejoin the RTP session or create a new one (if it was closed). This, in turn, will have whatever effects such rejoining or creating a session entails. For example, the SRTP rollover counter (ROC) will be reset, and the MG may start using a new SSRC value.

Regardless of the value of the *kleb* property, the MG shall neither receive nor send SRTP packets using an expired key (i.e., all such packets shall be discarded).

The MG's behaviour at key-exhaustion is completely independent of the expiry notification, and remains the same regardless of whether the *Master Key Expiry* event is configured at the stream level, termination level, or not at all.

6.6.4 Logging of security violations

Once an SRTP stream is established on a MG, sent and received packets are processed according to clause 3.3 of [IETF RFC 3711]. Received packets are authenticated and decrypted. During this process, received packets may be judged to have been replayed or may fail authentication and be discarded. In order to log these events, the MGC shall set the *Number of Replayed Packets* (*srtp/replay*) and the *Number of Authentication Failures* (*strp/authfail*) statistics. The MGC may audit these statistics when it wishes to know the number of replayed packets and/or authentication failures detected. If the MGC requires notification of such events, it shall use the Statistic Conditional Reporting package (see [ITU-T H.248.47]) with an appropriate reporting threshold.

7 Key management using SDP security descriptions

The MGC indicates that SDP security descriptions will be used for key management by setting the value of the *Key Management Scheme* property to "SDES". Under this scheme, the MGC and MG negotiate a Stream's SRTP parameter by placing a "crypto" SDP attribute in the Local and Remote Descriptors. The "crypto" attribute and its use for negotiating SRTP parameters is described in [IETF RFC 4568]. This clause provides additional details regarding the adaptation of those procedures for use with ITU-T H.248.

Naturally, this scheme is only applicable when SDP is used for the Local and Remote Descriptors. If the binary encoding of the protocol is used, the "crypto" SDP attribute can be carried using the SDP equivalents of clause C.11 of [ITU-T H.248.1]. The MG shall use error code 473 (Conflicting Property Values) when the Local and Remote Descriptors cannot carry a "crypto" SDP attribute and the *Key Management Scheme* is set to "SDES".

The Local Descriptor controls the SRTP parameters of the flow(s) sent by the MG. Similarly, the Remote Descriptor controls the SRTP parameters of the flow(s) received by the MG. A Local or Remote Descriptor indicates that the MG shall use SRTP to protect sent or received packets if both:

1) The media description ("m=" line) uses an SRTP-based profile as the transport protocol (e.g., "RTP/SAVP" or "RTP/SAVPF").

2) The SDP contains one or more "crypto" attributes.

If either of these conditions is not met, the MG shall not apply SRTP procedures to the packets. This Recommendation does not imply any special meaning to descriptors that match only one or none of these conditions.

The MG shall use error code 474 (Invalid SDP Syntax) if the above procedures indicate that the MG shall protect flows using SRTP but the "crypto" attribute does not match the SRTP-specific format, as described in clause 6 of [IETF RFC 4568].

In the following clauses, words appearing in `fixed-font` are references to specific ABNF rules from clause 9 of [IETF RFC 4568].

7.1 Overspecification of SRTP parameters and multiple keys

There are two possible ways for the MGC to specify more than one set of SRTP parameters within one SDP group:

1) Overspecify the "crypto" attribute by including more than one such attribute in the SDP group.

2) Include more than one `key-param` in one "crypto" attribute.

These two methods can be combined (i.e., include several "crypto" attributes in the SDP group, each including more than one `key-param`).

According to clause 7.1.5 of [ITU-T H.248.1], the behaviour of the MG when the "crypto" attribute is overspecified depends on the value of the *ReserveValue* property. If this value is false, the MG shall choose only one of the included "crypto" attributes and remove all others from the SDP group. Conversely, if *ReserveValue* is true, the MG shall reserve enough resources to support as many of the included "crypto" attributes as it can, and keep all those supported attributes in the descriptor.

A Remote Descriptor with more than one "crypto" attribute and/or more than one `key-param` within a "crypto" attribute indicates that the MG shall be prepared to accept packets protected using any of the master keys contained in the Descriptor. To achieve this, each key shall include a master key identifier (MKI) value and that value shall be unique. Any command resulting in one MKI value being mapped to more than one master key shall be rejected using error 473 (Conflicting Property Values).

A Local Descriptor with more than one "crypto" attribute indicates that the MG has reserved resources for all these attributes; however, only the first "crypto" attribute is used by the MG for protecting sent packets. As the MG does not use any of the other "crypto" attributes, different attributes may include identical MKI values (or not include MKI at all). Such configurations are often transient and exist while the session is being set up. An example for such a scenario is provided in item 1 of clause I.1.

NOTE 1 – Mandating the use of the first "crypto" attribute in the Local Descriptor allows re-keying an existing session. The MGC would:

a) Overspecify the Local Descriptor of the sender, adding a second, new "crypto" attribute.

b) Overspecify the Remote Descriptor of the receiver, adding the new "crypto" attribute.

c) Remove the first "crypto" attribute from the sender's Local Descriptor, leaving only the new attribute there.

A "crypto" attribute with more than one `key-param` appearing first in the Local Descriptor indicates that the different `key-param` sub-fields shall be used sequentially. The MG shall use the first `key-param` whose master key has not yet expired for protecting sent packets. Once a master key expires (due to the number of either SRTP or SRTCP packets sent), the MG shall start using the next `key-param` in the attribute. As, over the course time, all `key-param` sub-fields might be used, each shall include a MKI value and that value shall be unique.

NOTE 2 – The above procedures allow for the "automatic" re-keying of a stream upon key exhaustion, without the need for additional signalling messages.

7.2 Wildcarding of SRTP parameters

In addition to overspecification, many sub-fields of the "crypto" attribute may be wildcarded using the CHOOSE ("$") wildcard. When a sub-field is wildcarded, the MG shall choose a value for it based on the MG capabilities and local configuration. The exact procedures for doing so are outside the scope of this Recommendation.

Table 1 summarizes the guidelines for the sub-fields that may be wildcarded. Sub-fields that do not appear in the table cannot be wildcarded.

Table 1 – Wildcarding of SDP security descriptions

Sub-Field	Guidelines
`crypto-suite`	Wildcarding this sub-field mandates that `key-salt` is also wildcarded, as the MGC cannot know in advance the required key length.
`key-info`	Each part of `key-info` is wildcarded separately
`key-salt`	Can be wildcarded. It is impossible to wildcard only the key or the salt.
`lifetime`	Can be wildcarded.
`mki`	Only `mki-value` can be wildcarded (i.e., `mki-length` cannot). The MG shall choose the mki-value so that it is different from any other MKI appearing in the descriptor.
`kdr`	Can be wildcarded, using the form "KDR=$"
`fec-order`	Can be wildcarded, using the form "FEC_ORDER=$"
`fec-key`	The `key-params` part of the sub-field can be wildcarded, using the procedures for `key-info` above.
`wsh`	Can be wildcarded, using the form "WSH=$"

The MGC may combine overspecification and wildcarding, i.e., include in a descriptor multiple "crypto" attributes, where some of the attribute's subfields contain the CHOOSE wildcard.

7.3 Interoperability with offer/answer-based implementations

Under the SDP offer/answer procedures of [IETF RFC 4568], some of the SRTP parameters are considered "negotiated", meaning that the same parameter value must be used for both the sent and received RTP packets. The list of these parameters is:

1) `crypto-suite`

2) `UNENCRYPTED_SRTCP`

3) `UNENCRYPTED_SRTP`

4) `UNAUTHENTICATED_SRTP`

To increase interoperability with such offer/answer based implementations, whenever the MG needs to choose a value for one of those parameters (i.e., when overspecification or wildcarding is employed), it shall ensure that the same value is used in both the Local and Remote Descriptors. Using different values in the Local and Remote Descriptors for a "negotiated" parameter is only allowed when the request sent by the MGC explicitly prevents the use of the same value.

7.4 SDES and SRTP cryptographic contexts

With regard to the initialization and maintenance of SRTP crypto contexts, the MGC and MG shall follow the procedures of clauses 6.4 and 6.5 of [IETF RFC 4568]. In addition, the MGC and MG shall follow the procedures of clause 7 of [IETF RFC 4568], adapted to ITU-T H.248's use of SDP (which is different from the offer/answer model covered by that document). The following list highlights the points of those clauses that have the most significant impact on the MGC's and MG's behaviour.

1) The ROC of any newly created crypto context shall be initialized to zero.

2) The MG should choose an initial sequence number in the range of $0..2^{15}–1$ for any RTP stream associated with a newly created SRTP crypto context.

3) The MG shall choose different SSRC values for different RTP streams sharing the same master key.

4) The MG shall remove crypto-contexts using the same procedures as for SSRC removal from the member table, as described in [IETF RFC 3550].

5) If the MGC has wildcarded a master key, the MG shall choose a master key different from all other master keys it is currently using. In particular, a master key chosen for the Local or Remote Descriptor shall be different from any other master key appearing in the Local or Remote Descriptor of the same stream.

6) A command that changes the first "crypto" SDP attribute in the Local or Remote Descriptor shall create a new SRTP crypto context, which will be used by the MG for sending or receiving packets respectively. In particular, such a command shall reset the relevant ROC counter (Note 1).

   A change of a master key that does not involve a new "crypto" attribute (e.g., when multiple `key-param` sub-fields exist) shall not cause a new crypto context to be created, and the existing context shall be used (Note 2).

   NOTE 1 – A change of the first "crypto" attribute is considered as equivalent to sending a new master-key in a SDP offer/answer procedure. Therefore, the MG shall follow the requirements of clause 7.1.4 of [IETF RFC 4568]:

   "*... the offerer MUST include a new master key with the offer (and in so doing, it will be creating a new crypto context where the ROC is set to zero).*"

   NOTE 2 – A change of the master-key that does not involve a new "crypto" attribute is equivalent to re-keying the SRTP session without using an offer/answer exchange. Therefore the MG shall follow the requirements of clause 3.3.1 of [IETF RFC 3711]:

   "*After a re-keying occurs (changing to a new master key), the rollover counter always maintains its sequence of values, i.e., it MUST NOT be reset to zero.*"

7) The MGC should apply a new "crypto" SDP attribute to the Local Descriptor (and hence create a new local crypto context) whenever it changes the address or port used in that Descriptor.

7.5 Mapping of master keys for sent packets and received packets statistics

When SDP security descriptions are used for key management, each entry in the *Sent SRTP Packets Protected by Master Key* (*srpk*) and *Sent SRTCP Packets Protected by Master Key* (*scpk*) shall correspond to one of the master keys appearing in the first "crypto" SDP attribute of the Local Descriptor. The order of entries in the statistics shall match the order of keys in the "crypto" attribute.

In a similar manner, each entry in the *Received SRTP Packets Protected by Master Key* (*rrpk*) and *Received SRTCP Packets Protected by Master Key* (*rcpk*) statistics shall correspond to one of the master keys appearing in the first "crypto" attribute of the Remote Descriptor.

Changing the first "crypto" attribute of the Local or Remote Descriptors will cause the MG to discard the appropriate statistics values, and to start maintaining new ones.

8 Security considerations

SDP security descriptions do not provide any inherent authentication or encryption of the SRTP parameters carried in the Local and Remote Descriptors. Therefore, use of this key-management scheme is only appropriate when the ITU-T H.248 channel is secured through some other means (e.g., IPSec).

Appendix I

Example call flows

(This appendix does not form an integral part of this Recommendation)

I.1 Initial session setup using SDP security descriptions

In the following examples, tokens such as <key1> and <key2> indicate sequences of 240 bits, encoded as 40 base64 characters.

1) The MGC ADDs a new, SRTP-enabled, termination to MG1.

The *Key Management Scheme* is set to SDES, the transport protocol is RTP/SAVP and a "crypto" attribute appear in the Local Descriptor, indicating that the packets sent by MG1 should be protected using SRTP.

The Local Descriptor contains two "crypto" attributes and *ReserveValue* is true, meaning that MG1 should reserve resources for both, but only use the first. Note that the MKI value "1" is shared between the two attributes, which is allowed.

```
MGC to MG1:
MEGACO/3 [123.123.123.4]:55555
Transaction = 10003 {
    Context = $ {
        Add = $ {
            Media {
                TerminationState {
                    srtp/km = SDES
                },
                Stream = 1 {
                    LocalControl {
                        Mode = RecvOnly,
                        ReservedValue = ON
                    },
                    Local {
v=0
c=IN IP4 $
m=audio $ RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:$|2^20|1:4;inline:$|2^20|2:4
a=crypto:2 F8_128_HMAC_SHA1_80 inline:$|$|1:4
                    }
                }
            }
        }
    }
}
```

2) MG1 returns the `key-salt` sub-fields it has chosen as well as the `lifetime` of the AES_F8 key (these sub-fields were wildcarded in the request). The <key1>, <key2>, <key3> values must all be different from one another.

```
MG1 to MGC
MEGACO/3 [124.124.124.222]:55555
Reply = 10003 {
    Context = 2000 {
        Add = A4445 {
            Media {
                Stream = 1 {
                    Local {
v=0
o=- 2890844526 2890842807 IN IP4 124.124.124.222
s=-
t=0 0
c=IN IP4 124.124.124.222
m=audio 2222 RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:<key1>|2^20|1:4;inline:<key2>|2^20|2:4
a=crypto:2 F8_128_HMAC_SHA1_80 inline:<key3>|2^30|1:4
                    }
                }
            }
        }
    }
}
```

3) The MGC ADDs a new, SRTP-enabled termination to MG2.

The Remote Descriptor includes the crypto attributes returned by MG1. *ReserveValue* is false, indicating that MG2 should choose the first "crypto" SDP attribute it supports.

The `crypto-suite`, `key-salt`, `lifetime` and `mki-value` of the Local Descriptor are all wildcarded.

The *Master Key Expiry* event is enabled on the complete termination, indicating that the MGC should be first notified of an imminent master key exhaustion when the encryption key can only protect 10'000 additional SRTP packets or 50 additional SRTCP packets. Another notification will be made when the key is completely exhausted.

```
MGC to MG2:
MEGACO/3 [123.123.123.4]:55555
Transaction = 50003 {
    Context = $ {
        Add = $ {
            Media {
                TerminationState {
                    srtp/km = SDES
                },
                Stream = 1 {
                    LocalControl {
                        Mode = SendRecv
                        ; ReserveValue is false by default
                    },
                    Local {
v=0
c=IN IP4 $
m=audio $ RTP/SAVP 4
a=ptime:30
a=crypto:1 $ inline:$|$|$:4
                    },
                    Remote {
v=0
c=IN IP4 124.124.124.222
m=audio 2222 RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:<key1>|2^20|1:4;inline:<key2>|2^20|2:4
a=crypto:2 F8_128_HMAC_SHA1_80 inline<key3>|2^30|1:4
                    }
                }
            },
            Events = 1234 {
                srtp/mke { rtpw=10000, rtcpw=50 }
            }
        }
    }
}
```

4) MG2 chooses the first "crypto" attribute in the Remote Descriptor. In accordance with clause 7.3, it chooses for the Local Descriptor the same `crypto-suite` as the one now used in the Remote Descriptor.

```
MG2 to MGC:
MEGACO/3 [125.125.125.111]:55555
Reply = 50003 {
    Context = 5000 {
        Add = A5556{
            Media {
                Stream = 1 {
                    Local {
v=0
o=- 7736844526 7736842807 IN IP4 125.125.125.111
s=-
t=0 0
c=IN IP4 125.125.125.111
m=audio 1111 RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:<key4>|2^20|1:4
                    },
                    Remote {
v=0
o=- 7736849782 7736858112 IN IP4 125.125.125.111
s=-
t=0 0
c=IN IP4 124.124.124.222
m=audio 2222 RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:<key1>|2^20|1:4;inline:<key2>|2^20|2:4
                    }
                }
            }
        }
    }
}
```

5) The MGC updates MG1's Local and Remote Descriptors according to the choices made by MG2. The *Master Key Expiry* event is configured on the termination, using the same parameter values as the ones used at 3).

```
MGC to MG1:
MEGACO/3 [123.123.123.4]:55555
Transaction = 60006 {
    Context = 2000 {
        Modify = A4445 {
            Media {
                Stream = 1 {
                    LocalControl {
                        Mode = SendRecv
                    },
                    Local {
v=0
c=IN IP4 124.124.124.222
m=audio 2222 RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:<key1>|2^20|1:4;inline:<key2>|2^20|2:4
                    },
                    Remote {
v=0
c=IN IP4 125.125.125.111
m=audio 1111 RTP/SAVP 4
a=ptime:30
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:<key4>|2^20|1:4
                    },

                }
            },
            Events = 5678 {
                srtp/mke { rtpw=10000, rtcpw=50 }
            }
        }
    }
}
```

6) MG1 acknowledges the MODIFY request.

```
MG1 to MGC
MEGACO/3 [124.124.124.222]:55555
Reply = 60006 {
    Context = 2000 {
        Modify = A4445
    }
}
```

I.2 MG1's key is about to expire

1) MG1 sends a *Master Key Expiry* NOTIFY request to the MGC. The *Key Expired* parameter is missing and its default value (false) is used, indicating that the key has not yet expired, but that either the SRTP or SRTCP watermarks has been crossed.

```
MG1 to MGC:
MEGACO/3 [124.124.124.222]:55555
Transaction = 76819 {
    Context = 2000 {
        Notify = A4445 {
           ObservedEvents = 5678 {
                20091201T07450122:srtp/mke ;ke is false by default
            }
        }
    }
}
```

2) The MGC acknowledges the NOTIFY request.

```
MGC to MG1:
MEGACO/3 [123.123.123.4]:55555
Transaction = 76819 {
    Context = 2000 {
        Notify = A4445
    }
}
```

I.3 Auditing SRTP capabilities

1) The MGC audits all SRTP properties on MG1's Root termination.

```
MGC to MG1
MEGACO/3 [123.123.123.4]:55555
Transaction = 87395 {
  Context = - {
    AuditValue = Root {
      Audit { TerminationState { srtp/* } }
    }
  }
}
```

2) MG1 answers with the lists of encryption and authentication transforms that it supports. These lists are missing the NULL value, meaning that MG1's security policy does not allow the use of unencrypted or unauthenticated SRTP packets.

```
MG1 to MGC
MEGACO/3 [124.124.124.222]:55555
Reply = 87395 {
    Context = - {
        AuditValue = Root {
            TerminationState { srtp/set=[AES_CM_128, AES_CM_192, AES_CM_256],
                               srtp/sat=[HMAC_SHA1_32, HMAC_SHA1_80]
            }
        }
    }
}
```

I.4 Auditing of SRTP Statistics

1) The MGC audits the SRTP statistics of stream 1 on MG1:

```
MGC to MG1:
MEGACO/3 [123.123.123.4]:2944
Transaction = 91903 {
    Context = 2000 {
        AuditValue = A4445 {
            Audit {
                Media {
                    Stream = 1 {
                        Statistics { srtp/* }
                    }
                }
            }
        }
    }
}
```

2) MG1 returns the current SRTP statistics. According to the values returned, MG1 has discarded 7 packets due to authentication failure and considered 3 packets as replays. In addition (assuming that MG1 is using the keys negotiated in item 1 of clause I.1) the MG has protected 2^{20} SRTP packets and 4'086 SRTCP packets using <key1>, and 37'112 SRTP packets and 941 SRTCP packets using <key2>. It received 519'733 SRTP packets and 2080 SRTCP packets protected by <key4>.

```
MG1 to MGC:
MEGACO/3 [124.124.124.222]:55555
Reply = 91903 {
    Context = 2000 {
        AuditValue = A4445 {
            Media {
                Stream = 1 {
                    Statistics {
                        srtp/replay = 3,
                        srtp/authfail = 7,
                        srtp/srpk = [1048576, 37112],
                        srtp/scpk = [4086, 941],
                        srtp/rrpk = 519733,
                        srtp/rcpk = 2080
                    }
                }
            }
        }
    }
}
```

Appendix II

Sample use-cases of SRTP bearer encryption

(This appendix does not form an integral part of this Recommendation)

This appendix illustrates some network level scenarios that employ SRTP bearer encryption.

II.1 Use-case #1: ITU-T H.248 MG for peering IP and circuit-switched networks

Figure II.1 illustrates an ITU-T H.248 connection model of (IP, physical). This model is often employed for peering a circuit-switched and an IP network at a residential, access or trunking MG. The RTP session is terminated by the ITU-T H.248 MG. The MG is consequently behaving as a RTP end system (see clause 3 of [IETF RFC 3550]).

Any application of SRTP as a means for media security implies the termination of the SRTP session by the corresponding ITU-T H.248 stream.

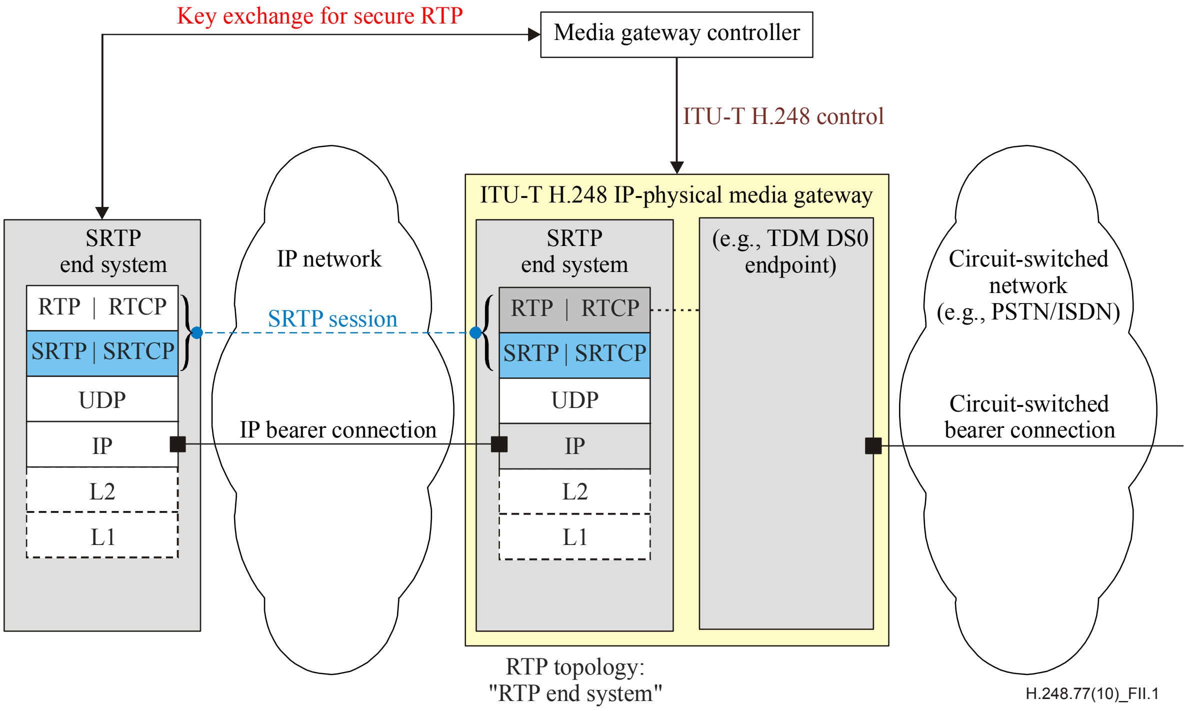


Figure II.1 – Use case #1: SRTP to circuit-switched ITU-T H.248 MG

II.2 Use case #2: ITU-T H.248 MG for peering IP networks

ITU-T H.248 IP-IP MGs are widely used as, e.g., border routers, border gateways, policy enforcement points, firewalls with session-dependent filter rules, NAT devices, media transcoders, etc.

Figure II.2 outlines a scenario, where such a gateway is located between two IP domains: one domain without any media security and another domain using SRTP encrypted media. The ITU-T H.248 MG behaves as two, back-to-back RTP end systems due to the termination of SRTP in one ITU-T H.248 stream.

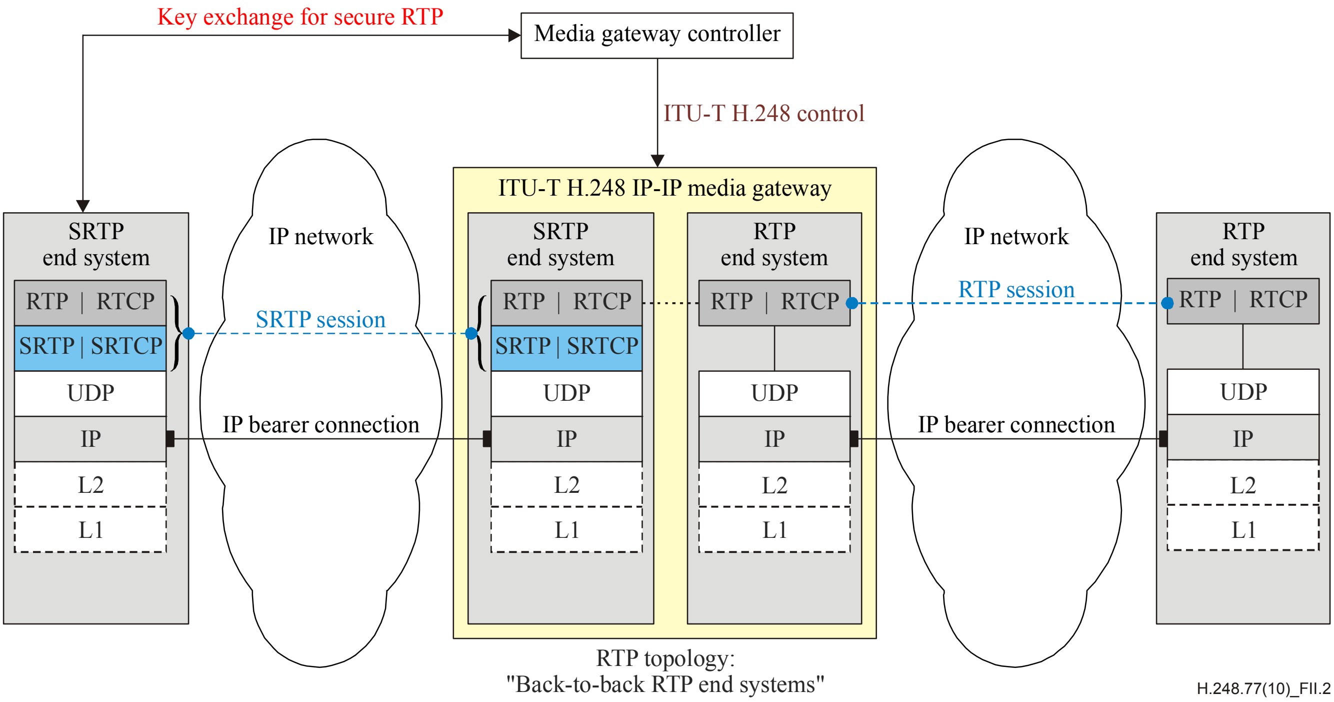
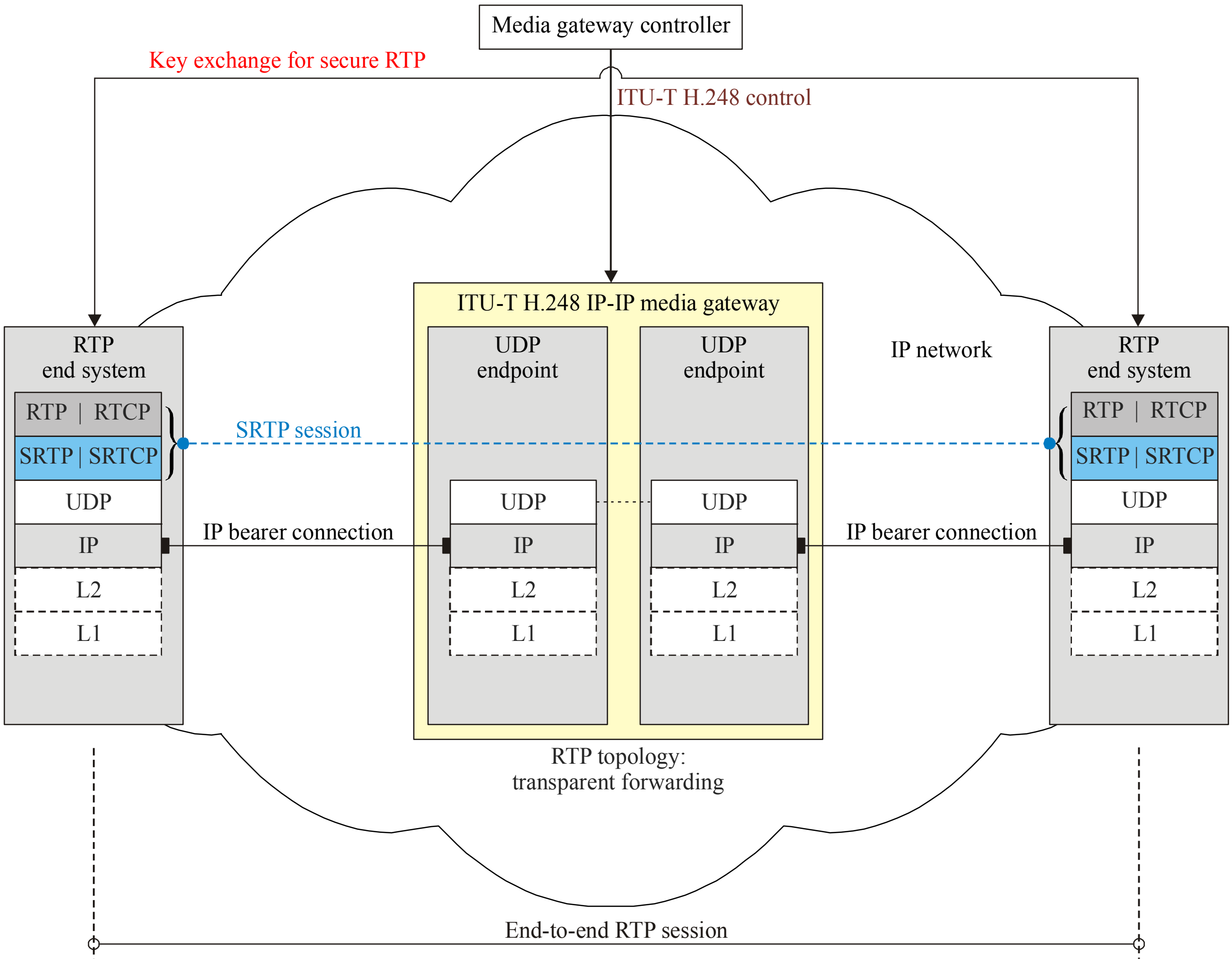


Figure II.2 – Use case #2: SRTP to RTP ITU-T H.248 MG

II.3 Use case #3: Transparent SRTP forwarding

It is possible for an MG to transparently forward SRTP packets, treating them as unprotected UDP or RTP packets. Such a scenario is illustrated in Figure II.3.

As stated in clause 1, this use-case is outside the scope of this Recommendation. It is presented here for the sake of completeness.



NOTE – The ITU-T H.248 MG may provide a local NAPT function, i.e., be media-agnostic, but transport-protocol aware (due to UDP checksum updates).

H.248.77(10)_FII.3

Figure II.3 – Use case #3: ITU-T H.248 MG with transparent SRTP forwarding

Bibliography

[b-IETF RFC 3264]	IETF RFC 3264 (2002), *An Offer/Answer Model with Session Description Protocol (SDP).*
[b-IETF RFC 4567]	IETF RFC 4567 (2006), *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011