International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.93

(10/2014)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: ITU-T H.248 support for control of transport security using the datagram transport layer security (DTLS) protocol

Recommendation ITU-T H.248.93

ITU-T

International Telecommunication Union

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
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Interoperability compliance testing of personal health systems (HRN, PAN, LAN and WAN)	H.820–H.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.248.93

Gateway control protocol: ITU-T H.248 support for control of transport security using the datagram transport layer security (DTLS) protocol

Summary

Datagram transport layer security (DTLS) is a session layer protocol for securing IP transport protocols. DTLS bearer plane traffic could be terminated or forwarded by ITU-T H.248 media gateways. DTLS is derived from the transport layer security (TLS) protocol. Recommendation ITU-T H.248.93 provides information for (DTLS) support by ITU-T H.248 entities with focus on the reuse of "ITU-T H.248 TLS packages" (according to Recommendation ITU-T H.248.90) for DTLS. This Recommendation defines an ITU-T H.248 package extension to the TLS capability negotiation package for the support of DTLS-SRTP sessions.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T H.248.93	2014-10-14	16	11.1002/1000/12244

Keywords

ITU-T H.248, DTLS, TLS.

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

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T H.248.93

Gateway control protocol:
ITU-T H.248 support for control of transport security using the datagram transport layer security (DTLS) protocol

1 Scope

Datagram transport layer security (DTLS) protocol [b-IETF RFC 4347] and [IETF RFC 6347] is derived and thus aligned with the transport layer security (TLS) protocol [IETF RFC 5246]. There are consequently many commonalities between the control of DTLS bearers and TLS bearers in ITU-T H.248 gateways.

ITU-T H.248-controlled TLS bearers are subject of [ITU-T H.248.90] and [ITU-T H.248.91].

The purpose of this Recommendation is to define usage of [ITU-T H.248.90] for DTLS bearers. It includes in particular:

– description of DTLS specific use cases;

– modelling information;

– description of MG bearer plane differences between DTLS and TLS;

– usage of TLS-defined ITU-T H.248 packages for DTLS bearer types; and

– an extension package for the specific application of DTLS-SRTP [IETF RFC 5764].

Appendix I provides a non-exhaustive list of example use cases for DTLS in two slightly different areas of applications:

1. DTLS as "transport security" means for "DTLS-over-L4" or "L4-over-DTLS" IP bearer traffic; and
2. DTLS as "key exchange" means for RTP/L4/IP bearer traffic using media security according to the secure real-time transport protocol (SRTP).

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.248.88]	Recommendation ITU-T H.248.88 (2014), *Gateway control protocol: RTP topology dependent RTCP handling by ITU-T H.248 media gateways with IP terminations*.
[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.248.91]	Recommendation ITU-T H.248.91 (2014), *Gateway control protocol: Guidelines on the use of ITU-T H.248 capabilities for transport security in TLS networks in ITU-T H.248 profiles*.

[ITU-T H.248.92] Recommendation ITU-T H.248.92 (2014), *Gateway control protocol: Stream endpoint interlinkage package*.

[ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1: 1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[IETF RFC 4572] IETF RFC 4572 (2006), *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 term defined elsewhere:

3.1.1 transparent forwarding [ITU-T H.248.88]: MG packet forwarding behaviour with the characteristic of *Lx-PDU integrity*. This is a unidirectional characteristic of a Lx-PDU flow.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 DTLS transparent forwarding: MG packet forwarding behaviour with the characteristic of *DTLS-PDU integrity* (Notes 1 and 2). This is a unidirectional characteristic of a DTLS-PDU flow.

NOTE 1 – A DTLS PDU relates to a DTLS message in [IETF RFC 5246].

NOTE 2 – Definition based on clause 3.1.1, i.e., the characteristic of *PDU integrity* comprises the properties of *bit integrity* and *data integrity* (see also clauses 3.1.1, 3.1.2 and 3.2.3 in [ITU-T H.248.88]).

NOTE 3 – There is the characteristic of *DTLS message integrity* in the context of "DTLS transparent forwarding". The MG might be DTLS aware; e.g., support of DTLS related statistics or event detection would not violate transparent forwarding behaviour.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

B2BIH	Back-to-Back IP Host
DCCP	Datagram Congestion Control Protocol
DTLS	Datagram Transport Layer Security
EP	Endpoint
IFP	Internet Facsimile Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
L3	Layer three

L4	Layer four
L4+	Above layer four
MAC	Message Authentication Code
MG	Media Gateway
MGC	Media Gateway Controller
MKI	Master Key Identifier
PSTN	Public Switched Telephone Network
RTP	Real-time Transport Protocol
SCTP	Stream Control Transmission Protocol
SDES	SDP security Descriptions
SDP	Session Description Protocol
SEP	Stream Endpoint
SEPP	Stream Endpoint Pair
SIP	Session Initiation Protocol
SRTP	Secure RTP
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPKT	Transport Protocol Data Unit Packet
UDP	User Datagram Protocol
UDPTL	(Facsimile) UDP Transport Layer (protocol)
WebRTC	Web-based Real-Time Communication= Real-Time Communication in WEB-browsers (as work item in W3C)

5 Conventions

5.1 Conventions used in signalling flows

The following conventions are used in the example signalling flows:

L4 Est.req L4 Est.ack	Abstracted (protocol-independent) representation for establishment requests/acknowledgements of new connection-oriented IP transport connections.
L4 Rel.req L4 Rel.ack	Abstracted (protocol-independent) representation for release requests/acknowledgements of existing connection-oriented IP transport connections.
DTLS Est.req DTLS Est.ack	Abstracted (DTLS message/procedure independent) representation for establishment requests/acknowledgements of new DTLS security sessions.
DTLS Rel.req DTLS Rel.ack	Abstracted (protocol-independent) representation for release requests/acknowledgements of existing DTLS security sessions.

5.2 DTLS endpoint notations

The notion of endpoint represents different concepts, which are illustrated in Figure 1.

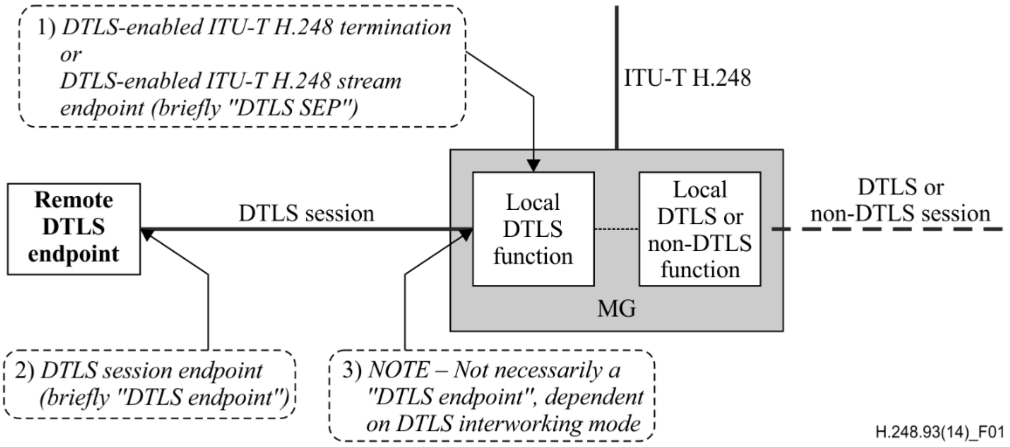

1) DTLS-enabled ITU-T H.248 termination
or
DTLS-enabled ITU-T H.248 stream endpoint (briefly "DTLS SEP")
ITU-T H.248
Remote DTLS endpoint
DTLS session
Local DTLS function
Local DTLS or non-DTLS function
DTLS or non-DTLS session
MG
2) DTLS session endpoint (briefly "DTLS endpoint")
3) NOTE – Not necessarily a "DTLS endpoint", dependent on DTLS interworking mode
H.248.93(14)_F01

Figure 1 – Conventions for DTLS endpoint types

Usage in:

- *ITU-T H.248 control*: ITU-T H.248 terminations/stream endpoint with DTLS processing are denoted as DTLS-enabled termination or stream endpoint (SEP) respectively;
- *user plane* (DTLS): a *DTLS bearer connection endpoint* represents an "(N)-connection-endpoint" according to [ITU-T X.200]. This concept comprises a *terminator* (i.e., DTLS protocol termination) plus a *service access point* (i.e., L4+ access). Furthermore, DTLS is a client/server type of protocol; a "DTLS endpoint" provides thus either a *client* or *a server* role.

The stream endpoints (SEP) subject of the packages and procedures of this Recommendation may act as a DTLS bearer connection endpoint or not:

- The basic session control package (for DTLS, see clause 8), the capability negotiation package (for DTLS, see clause 10) and the session maintenance package (for DTLS, see clause 12) are related to [ITU-T H.248.90], hence assumes a SEP that is a DTLS bearer connection endpoint.
- The traffic volume metrics package (for DTLS, see clause 13) (related to [ITU-T H.248.90]) is applicable both for SEPs that are DTLS bearer connection endpoints and SEPs which are not.
- The usage of the Stream endpoint interlinkage package [ITU-T H.248.92] for DTLS (see clause 9) assumes a SEP that is a DTLS bearer connection endpoint.
- The DTLS extended capabilities package (see clause 11) assumes a SEP that is a DTLS bearer connection endpoint.

6 Use case descriptions

Transport security is a network level service and primarily affects ITU-T H.248 media gateways (MGs). Basic use cases may be identified from the perspective of:

- ITU-T H.248 MG type: IP-to-IP gateway (see clause 6.2) or IP-to-non-IP gateway (see clause 6.3) in case of usual two-party communication services; and
- Multiparty service types (see clause 6.4).

It may be noted that the various network use cases may be abstracted by a single bearer connection model, see clause 7.2.

6.1 Use cases related to DTLS transport modes

The DTLS protocol is independent of the underlying transport protocol stack and multiple DTLS transport modes are possible (see Figure 2).

This Recommendation does not depend on any DTLS transport mode, although it uses DTLS-over-UDP/IP as example.

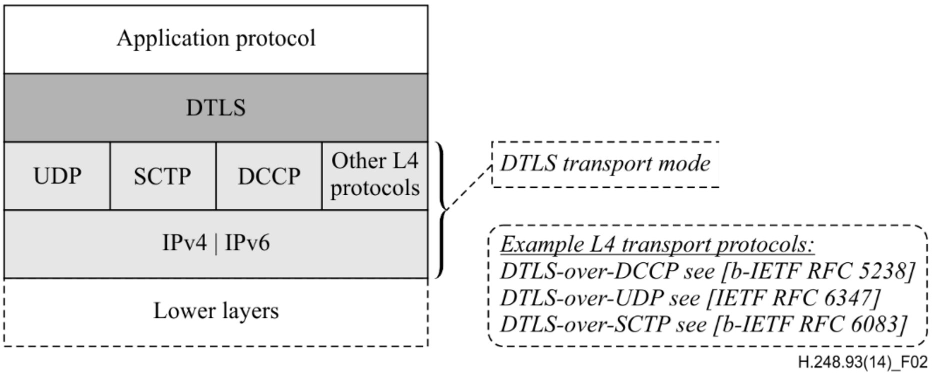

Application protocol
DTLS
UDP
SCTP
DCCP
Other L4 protocols
IPv4 | IPv6
Lower layers
DTLS transport mode
Example L4 transport protocols:
DTLS-over-DCCP see [b-IETF RFC 5238]
DTLS-over-UDP see [IETF RFC 6347]
DTLS-over-SCTP see [b-IETF RFC 6083]
H.248.93(14)_F02

Figure 2 – DTLS transport modes

6.2 Bearer connection network use cases with ITU-T H.248 IP-IP gateways

6.2.1 High-level use case categories

The notion "IP-to-IP" (briefly "IP-IP") indicates an *(IP, IP) connection model* (as part of clause 6.4 in the profile definition template (see Appendix III in [ITU-T H.248.1])).

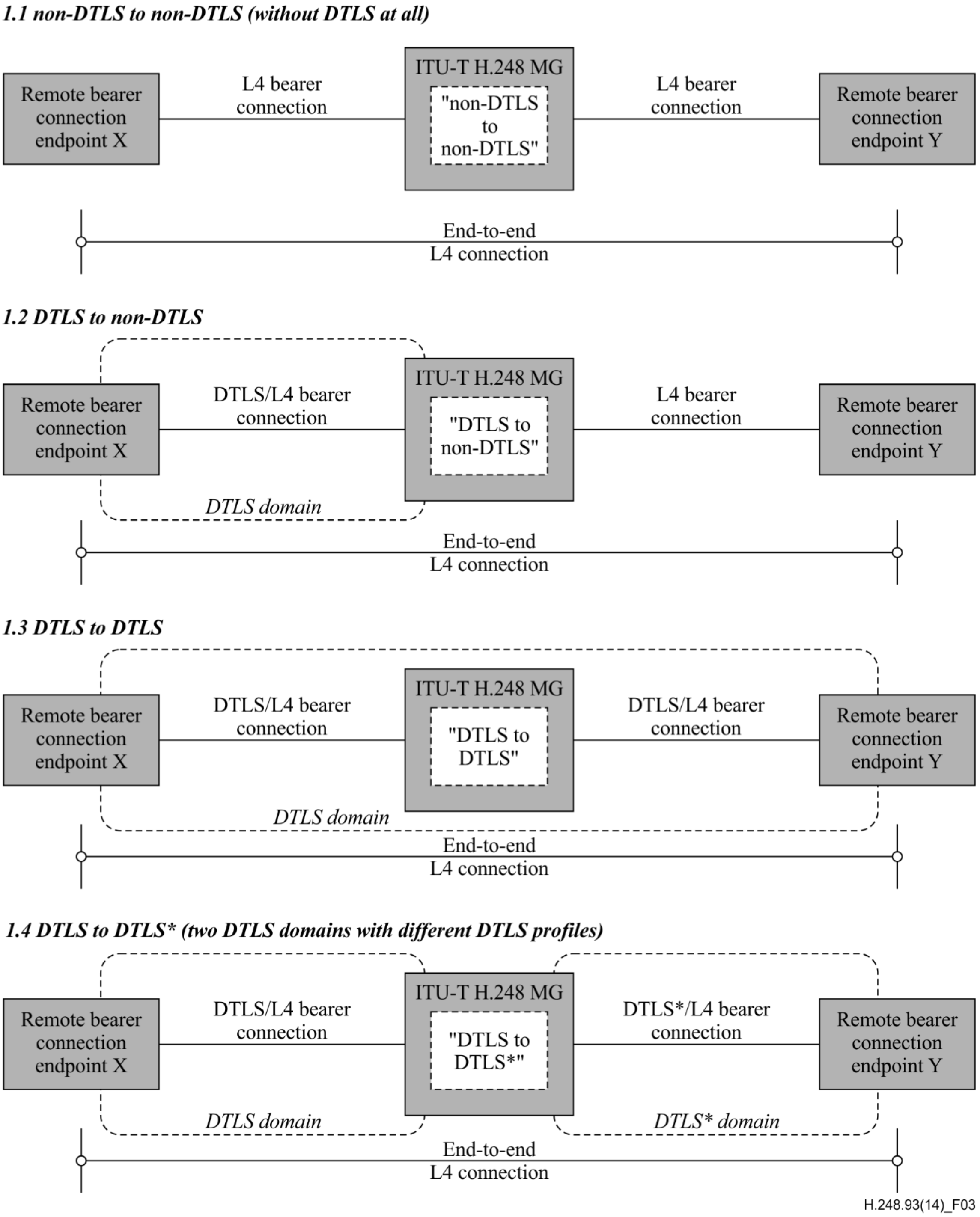
Each ITU-T H.248 stream endpoint (SEP) may be associated with a non-DTLS or different DTLS protocol stack variants, leading to various bearer network connection use cases (see Figure 3):

– **Use case 1.1**: an ITU-T H.248 IP-IP MG located in the middle of an end-to-end L4 connection without any applied transport security (abbreviated as "non-DTLS to non-DTLS");

– **Use case 1.2**: an end-to-end L4 connection traversing two network domains with different transport security policies ("DTLS", "no DTLS"). The ITU-T H.248 IP-IP MG is located in the middle, at the border of both domains (abbreviated as "DTLS to non-DTLS");

– **Use case 1.3**: an ITU-T H.248 IP-IP MG located in the middle of an end-to-end L4 connection with applied transport security (abbreviated as "DTLS to DTLS");

– **Use case 1.4**: there is end-to-end transport security, but different DTLS profiles (abbreviated as "DTLS to DTLS*").



1.1 non-DTLS to non-DTLS (without DTLS at all)
Remote bearer connection endpoint X
L4 bearer connection
ITU-T H.248 MG
"non-DTLS to non-DTLS"
L4 bearer connection
Remote bearer connection endpoint Y
End-to-end L4 connection
1.2 DTLS to non-DTLS
Remote bearer connection endpoint X
DTLS/L4 bearer connection
ITU-T H.248 MG
"DTLS to non-DTLS"
L4 bearer connection
Remote bearer connection endpoint Y
DTLS domain
End-to-end L4 connection
1.3 DTLS to DTLS
Remote bearer connection endpoint X
DTLS/L4 bearer connection
ITU-T H.248 MG
"DTLS to DTLS"
DTLS/L4 bearer connection
Remote bearer connection endpoint Y
DTLS domain
End-to-end L4 connection
1.4 DTLS to DTLS* (two DTLS domains with different DTLS profiles)
Remote bearer connection endpoint X
DTLS/L4 bearer connection
ITU-T H.248 MG
"DTLS to DTLS*"
DTLS*/L4 bearer connection
Remote bearer connection endpoint Y
DTLS domain
DTLS* domain
End-to-end L4 connection
H.248.93(14)_F03

Figure 3 – Bearer connection network use cases with ITU-T H.248 IP-IP gateways

6.2.2 Use case variations

6.2.2.1 DTLS-to-DTLS transparent forwarding

This scenario is a variation of use case 1.3 (clause 6.2.1) and requires the MG behaviour of DTLS transparent forwarding according to clause 3.2.1.

6.3 Bearer connection network use cases with DTLS transport mode change

The L4 transport protocol could change, e.g., an ITU-T H.248 MG enabled for DTLS/UDP to DTLS/DCCP interworking.

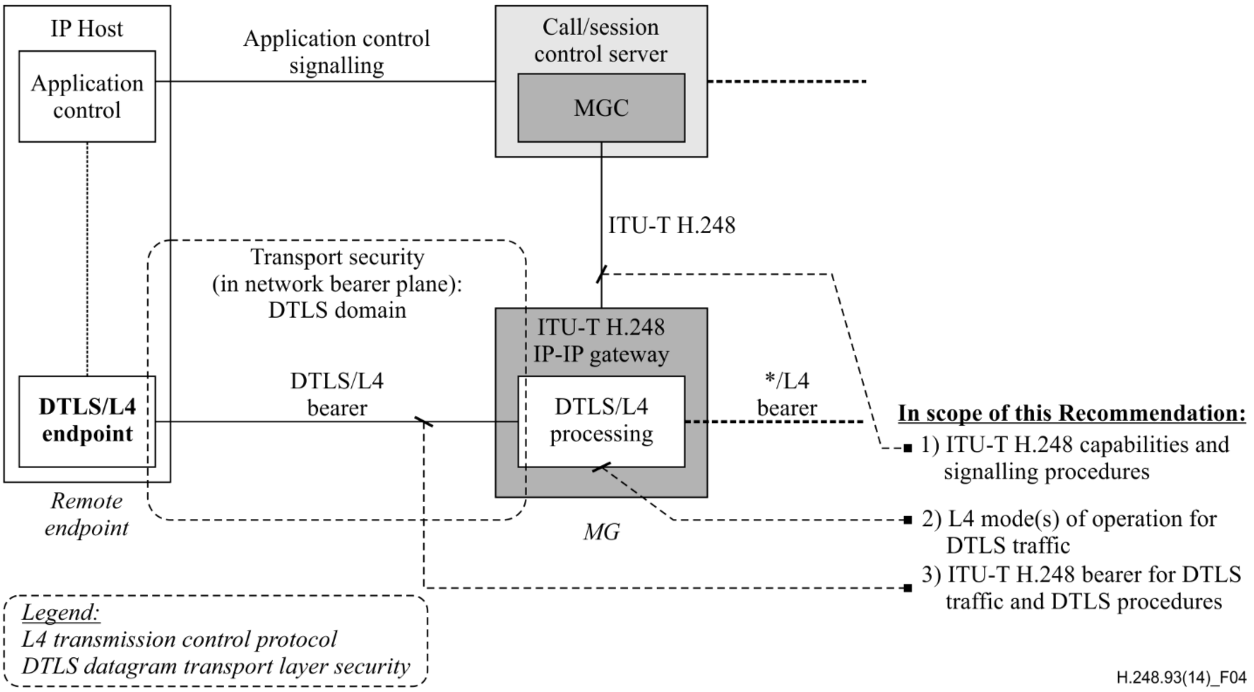
6.4 Bearer connection network use cases with multiparty services

A multiparty communication service leads to connection models with more than two ITU-T H.248 terminations. Such gateway topologies provide normally application aware type of functions (e.g., as media server), thus DTLS sessions would be terminated by the MG. It results in a type of "DTLS to DTLS*" interworking, such as use case 1.4 (clause 6.2.1).

7 Models

7.1 Network model from ITU-T H.248 entity point of view

The network model depicted in Figure 4 illustrates the relevant areas covered by this Recommendation. The ITU-T H.248 MG peers with a DTLS-capable IP host remote endpoint. Both DTLS endpoints span a network transport security domain (here DTLS domain).


IP Host
Application control
Application control signalling
Call/session control server
MGC
ITU-T H.248
Transport security (in network bearer plane): DTLS domain
ITU-T H.248 IP-IP gateway
DTLS/L4 bearer
*/L4 bearer
DTLS/L4 endpoint
DTLS/L4 processing
Remote endpoint
MG
In scope of this Recommendation:
1) ITU-T H.248 capabilities and signalling procedures
2) L4 mode(s) of operation for DTLS traffic
3) ITU-T H.248 bearer for DTLS traffic and DTLS procedures
Legend:
L4 transmission control protocol
DTLS datagram transport layer security
H.248.93(14)_F04

NOTE – There might be an additional network interface in case of dedicated, centralized network servers in the DTLS domain with respect to key distribution (such as key management systems). Such kinds of interfaces are out of scope of this Recommendation.

Figure 4 – Network model from ITU-T H.248 entity point of view ("half call/bearer connection model")

This Recommendation addresses primarily:

– signalling capabilities and procedures at the ITU-T H.248 interface;

– aspects and control of DTLS level mode(s) of operation in the ITU-T H.248 MG; and

– configuration and procedures of the DTLS/L4/IP protocol stack for ITU-T H.248-controlled bearers.

7.2 Bearer connection model

Figure 5 provides the L4/IP protocol stack with the suite of DTLS protocols and their sub-layer organization.

Figure 6 details the generic connection-model where a DTLS-enabled termination is connected to a single other termination (either DTLS-enabled or not). The generalization to any number of terminations is trivial.

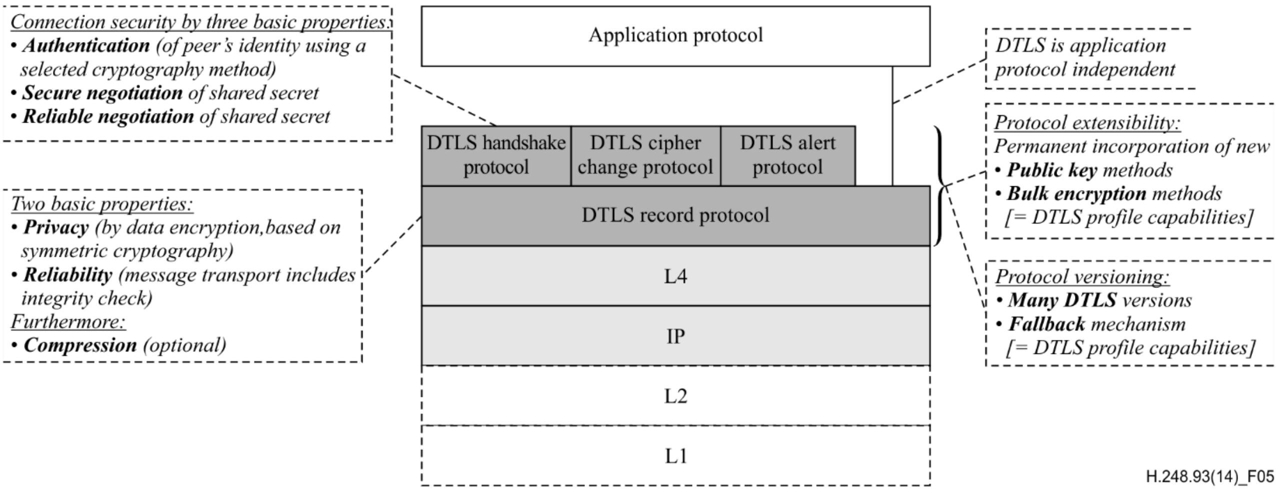

Connection security by three basic properties:
• Authentication (of peer's identity using a selected cryptography method)
• Secure negotiation of shared secret
• Reliable negotiation of shared secret
Two basic properties:
• Privacy (by data encryption,based on symmetric cryptography)
• Reliability (message transport includes integrity check)
Furthermore:
• Compression (optional)
Application protocol
DTLS handshake protocol
DTLS cipher change protocol
DTLS alert protocol
DTLS record protocol
L4
IP
L2
L1
DTLS is application protocol independent
Protocol extensibility:
Permanent incorporation of new
• Public key methods
• Bulk encryption methods
[= DTLS profile capabilities]
Protocol versioning:
• Many DTLS versions
• Fallback mechanism
[= DTLS profile capabilities]
H.248.93(14)_F05

Figure 5 – L4/IP protocol stack with DTLS protocol

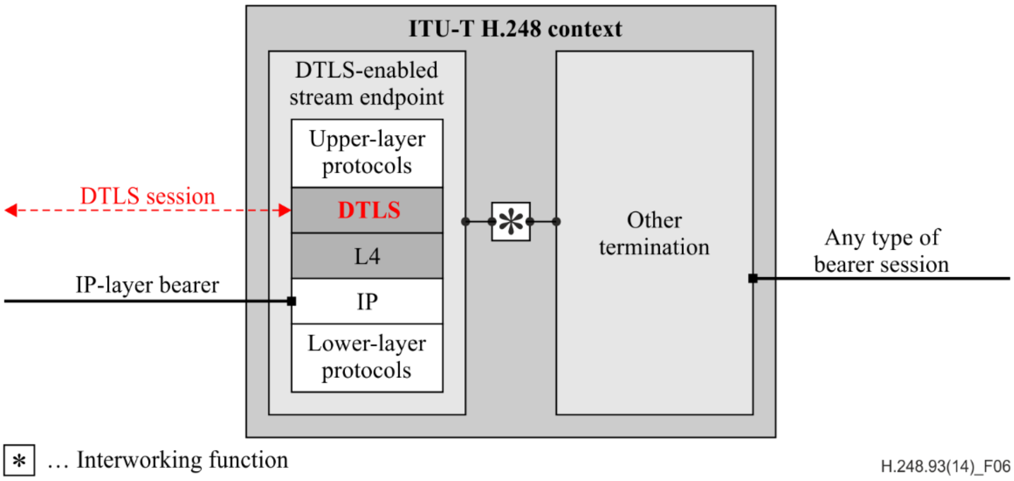


Figure 6 – Two-termination context with a DTLS termination

8 Basic session control package (for DTLS)

Table 1 summarizes the relevant aspects.

Table 1 – Basic session control package (for DTLS)

Reusable ITU-T H.248 package?	Yes, the "TLS basic session control package" (*tlsbsc*) according to [ITU-T H.248.90] shall be used for DTLS.
ITU-T H.248: DTLS specific differences versus TLS?	No. The same state model applies, see Annex A. The DTLS protocol internal procedural differences are not visible from ITU-T H.248 interface perspective, with regards to the basic blocking, establishment and release of a DTLS session.
Limitations, modifications or special considerations?	None.
Further comments?	DTLS supports additional protocol extensions (e.g., sequence numbers, timers) in order to address unreliable L4 transport protocols. Thus, DTLS itself provides an assured communication service, without any impact on the ITU-T H.248 interface.

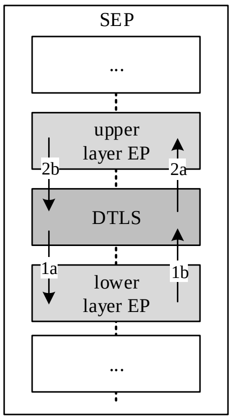
9 DTLS-specific stream endpoint interlinkage procedures

Table 2 summarizes the relevant aspects.

Table 2 – DTLS-specific stream endpoint interlinkage procedures

Reusable ITU-T H.248 package?	Yes, the "Stream endpoint interlinkage package" (seplink) according to [ITU-T H.248.92] shall also be basically used for DTLS.
ITU-T H.248: DTLS specific differences versus TLS?	Yes. 1. DTLS transport modes (see clause 6.1): The interlinkage between DTLS and the underlying L4 protocol is limited, actually L4 protocol dependent (due to support of connectionless (UDP) and connection-oriented (SCTP, DCCP) L4 protocols). 2. DTLS position in IP protocol stacks: The DTLS layer could be located on top of an L4 transport protocol (as usual), but also vice versa according to existing DTLS applications. Table 3 indicates the principle intra-SEP interlinkage options.
Limitations, modifications or special considerations?	None.
Further comments?	None.

Table 3 – Intra-SEP interlinkage options for DTLS



Intra-SEP interlinkage options for DTLS		
No.	**<source transport EP>**	**<interlinked transport EP>**
1a	DTLS	lower layer EP
1b	lower layer EP	DTLS
2a	DTLS	upper layer EP
2b	upper layer EP	DTLS

10 Capability negotiation package (for DTLS)

Table 4 summarizes the relevant aspects.

Table 4 – Capability negotiation package (for DTLS)

Reusable ITU-T H.248 package?	Yes, the "TLS capability negotiation package" (*tlscn*) according to [ITU-T H.248.90] shall be used for DTLS.
ITU-T H.248: DTLS specific differences versus TLS?	No for native DTLS sessions. The DTLS protocol internal procedural differences are not visible from ITU-T H.248 interface perspective. Yes for DTLS-SRTP sessions. There are DTLS protocol extensions in case of DTLS-SRTP [IETF RFC 5764] (see clause I.4.1), leading to additional ITU-T H.248 elements for (related "DTLS-SRTP protection profiles" and "SRTP Master Key Identifier". See clause 11.
Limitations, modifications or special considerations?	None.
Further comments?	None.

11 DTLS extended capabilities package

Package name: DTLS extended capabilities package

Package ID: dtlscn (0x011e)

Description: Native DTLS sessions may be negotiated solely on the basis of package *tlscn* (as base package) according to [ITU-T H.248.90].

DTLS sessions for the purpose of key exchange for SRTP sessions, so called DTLS-SRTP [IETF RFC 5764], need the consideration of additional (D)TLS protocol parameters.

Version: 1

Extends: tlscn (0x0118) version 1

11.1 Properties

11.1.1 DTLS-SRTP protection profiles

Property name: DTLS-SRTP protection profiles

Property ID: dspp (0x0009)

Description: This property indicates the protection profiles for DTLS-SRTP, according to section 4.1.2 of [IETF RFC 5764] "SRTP Protection Profiles" and their precedence (in descending order of preference) for the negotiation with the remote DTLS endpoint.

Type: Sublist of String

Possible values: Each string consists of four hexadecimal digits and represents the SRTP protection profile in accordance with the *DTLS-SRTP Protection Profiles* registry of IANA (http://www.iana.org/assignments/srtp-protection/srtp-protection.xhtml#srtp-protection-1).

The first value of the value pair as defined by the IANA registry shall be coded into the first two characters, and the second value shall be coded into the last two characters of the string. Thus, each value in its hexadecimal representation shall be converted into the double-hexdigit string. The "0x" shall be omitted and if needed, a "0" is used for padding.

Over-decadic digits are to be represented by lower case characters ("a".."f").

Default: Provisioned

NOTE – A particular DTLS protocol version may define default value(s). Thus, an ITU-T H.248 profile that defines a default version for DTLS could also specify default value(s) for this property.

Defined in: LocalControl (ephemeral IP terminations),
TerminationState (Root termination)

Both methods shall be mutually exclusive in this package version.

Characteristics: Read/Write

11.1.2 Master Key Identifier usage

Property name: Master Key Identifier usage

Property ID: mkiu (0x000a)

Description: This property indicates the use or not use of the DTLS-SRTP specific Master Key Identifier (MKI) (according to [IETF RFC 5764], clause 4.1.3 "srtp_mki value").

Type: Boolean

Possible values: False MKI shall not be used

True MKI shall be used

Default: Provisioned

Defined in: LocalControl (ephemeral IP terminations),
TerminationState (Root termination)

Both methods shall be mutually exclusive in this package version.

Characteristics: Read/Write

11.2 Events

None.

11.3 Signals

None.

11.4 Statistics

None.

11.5 Error codes

None.

11.6 Procedures

11.6.1 Extension versus base package

This extension package would typically be used in conjunction with the base package "*tlscn*" (clause 10 of [ITU-T H.248.90]), however, it could be also applied exclusively when all base package elements would use a default or provisioned value.

11.6.2 Principles of capability negotiations

The same principles as of the base package (clauses 10.6.1 to 10.6.3 of [ITU-T H.248.90]) apply for the extension package.

11.6.3 DTLS protocol parameter "DTLS-SRTP protection profiles"

Property *dspp* defines an additional ITU-T H.248 signalling element for the support of the DTLS protocol and shall be used in alignment with clause 10.6.6 of [ITU-T H.248.90]. It has to be noted that there are no interactions with the base package properties because the DTLS protocol extension parameter "DTLS-SRTP protection profiles" is orthogonal to the (D)TLS protocol parameter "TLS Cipher Suites" (see clause 10.1.3 of [ITU-T H.248.90]).

11.6.4 DTLS protocol parameter "Master Key Identifier"

11.6.4.1 Usage for DTLS-SRTP bearers

Property *mkiu* defines an additional ITU-T H.248 signalling element for the support of the Master Key Identifier (MKI) for DTLS-SRTP. The `srtp_mki` parameter is part of the DTLS `UseSRTPData` object (together with parameter `SRTPProtectionProfiles`, see clause 11.6.3), and the `srtp_mki` value contains the SRTP Master Key Identifier (MKI) value (if any) that the client will use for the SRTP packets. If this field has zero length, then no MKI will be used.

Usage of an MKI or not for a particular DTLS-SRTP session is not indicated at call control signalling (such as SIP/SDP). Signalling property *mkiu* at the ITU-T H.248 interface from media gateway controller (MGC) to MG would be thus based on a MGC-local policy.

11.6.4.2 Comparison of DTLS-SRTP and SDES-SRTP methods

The MKI for SRTP is transferred along the media-path in case of DTLS-SRTP, or transferred via the signalling path (session initiation protocol (SIP), ITU-T H.248) in case of SDES-SRTP [b-IETF RFC 4568]:

– SDES-SRTP uses [b-ITU-T H.248.77] in combination with the session description protocol (SDP) "a=crypto:" attribute. The MKI in this case is a SDP attribute parameter.

– DTLS-SRTP uses this Recommendation (i.e., the SDP "a=crypto:" attribute is not used).

These methods are mutually exclusive, and an ITU-T H.248-controlled SRTP stream endpoint will only use one option.

12 Session maintenance package (for DTLS)

Table 5 summarizes the relevant aspects.

Table 5 – Session maintenance package (for DTLS)

Reusable ITU-T H.248 package?	Yes, the "TLS session maintenance package" (*tlsm*) according to [ITU-T H.248.90] shall be used for DTLS.
ITU-T H.248: DTLS specific differences versus TLS?	No. There might be different alerts, but the DTLS protocol internal procedural differences do not impact the ITU-T H.248 package design.
Limitations, modifications or special considerations?	None.
Further comments?	None.

13 Traffic volume metrics package (for DTLS)

Table 6 summarizes the relevant aspects.

Table 6 – Traffic volume metrics package (for DTLS)

Reusable ITU-T H.248 package?	Yes, the "TLS traffic volume metrics package" (*tlstv*) according to [ITU-T H.248.90] shall be used for DTLS.
ITU-T H.248: DTLS specific differences versus TLS?	No. The TLS data model could be reused for DTLS (see Annex B).
Limitations, modifications or special considerations?	None.
Further comments?	None.

14 Package-less DTLS control

14.1 Related to DTLS authentication

The SDP "a=fingerprint:" attribute (according to [IETF RFC 4572]) shall be used according to clause 13.2 of [ITU-T H.248.90].

Annex A

State modelling for DTLS bearer connection endpoints

(This annex forms an integral part of this Recommendation.)

The same state model as for TLS applies for DTLS, see clause A.3 of [ITU-T H.248.90].

Annex B

DTLS protocol layer: Data model

(This annex forms an integral part of this Recommendation.)

The same data model as for TLS applies for DTLS, see Annex B of [ITU-T H.248.90].

Appendix I

Sample use cases of DTLS bearer encryption

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

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

I.1 Use cases for "application protocol agnostic DTLS handling"

The MG is unaware of the IP application protocol carried by DTLS packets. There are some basic interworking modes (see Figure I.1), from the perspective of user datagram protocol (UDP) and transmission control protocol (TCP) based data transports:

– **Use case I.1.1**: MG provides interworking between "DTLS/UDP/IP" and "TCP/IP";

– **Use case I.1.2**: MG provides interworking between "DTLS/UDP/IP" and "TLS/TCP/IP"; and

– **Use case I.1.3**: MG provides interworking between "(DTLS/)UDP/IP" and "(DTLS/)UDP/IP" in DTLS transparent forwarding mode.

I.2 Use cases for "DTLS-based transport security for facsimile packet relay service ITU-T T.38"

The IP application protocol is given by [b-ITU-T T.38], which relates to the Internet facsimile protocol (IFP) plus an underlying application level framing protocol such as UDP transport layer (UDPTL).

Background

[b-ITU-T T.38] defines three transport modes (ITU-T T.38 over UDPTL/UDP, RTP/UDP or TPKT/TCP), but does not provide any recommendation which mode should be selected when integrity and confidentiality protection is required.

Use case "ITU-T T.38-over-UDPTL/DTLS/UDP" relates to the UDPTL transport mode and is characterized by following aspects:

– the MG type would follow either a PSTN-to-IP connection model, such as access or trunking gateways in public switched telephone network (PSTN) emulation solutions, or an IP-to-IP connection model in case of ITU-T T.38 interworking according [b-ITU-T V.153];

– such a network configuration relates, for both connection models, to the "DTLS to non-DTLS" interworking case (see clause 6.2.1);

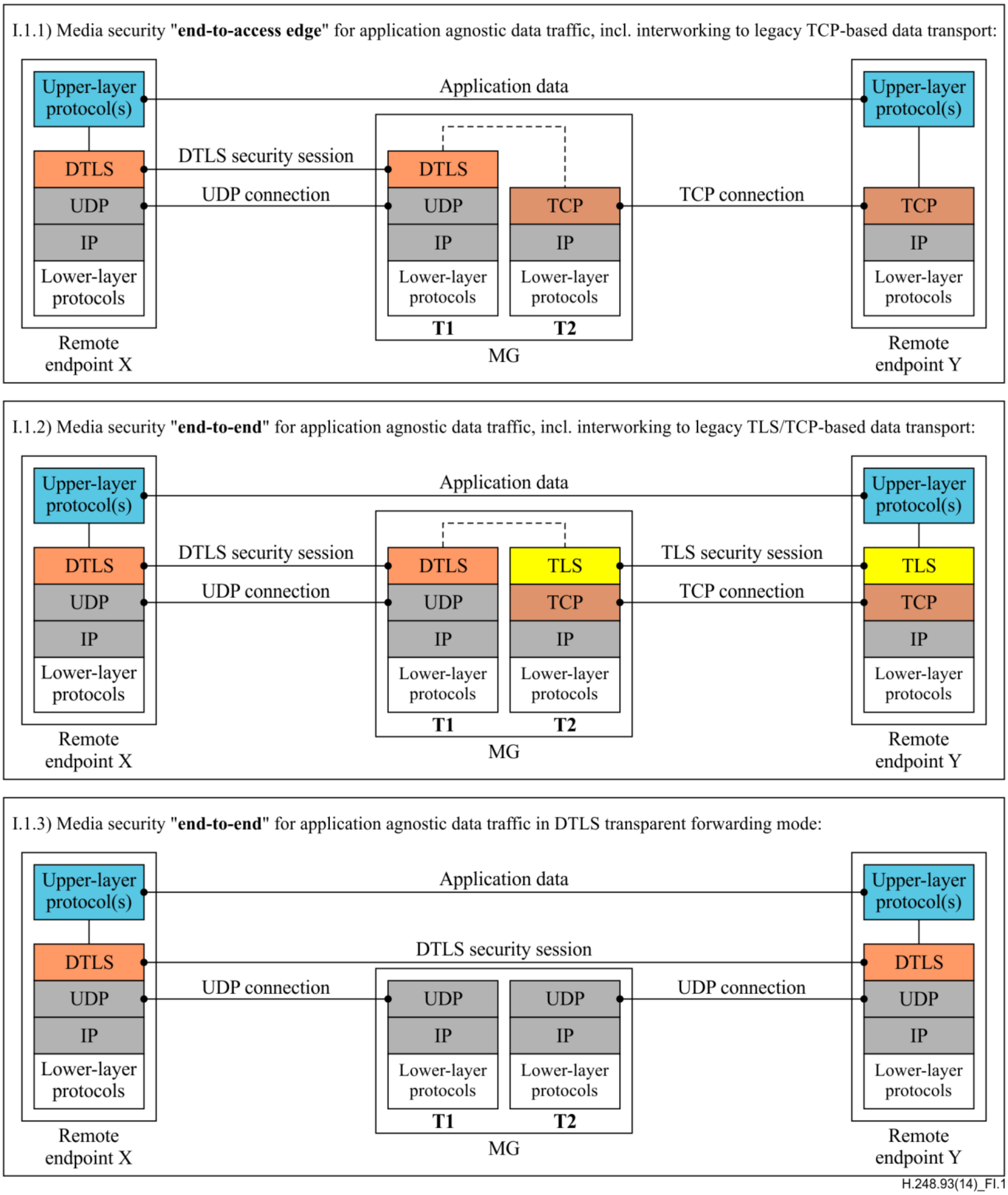
– UDP transport implies DTLS.

There are two principal use cases in case of end-to-end UDP based transport (see Figure I.2):

– use case I.2.1: MG provides interworking between "DTLS/UDP/IP" and "UDP/IP"; and

– use case I.2.2: MG provides interworking between "(DTLS/)UDP/IP" and "(DTLS/)UDP/IP" in DTLS transparent forwarding mode ("thus, similar as use case I.1.3").

It should be noted that the MG is not aware of the IP application protocol, hence it is also not aware of the "UDPTL" protocol. Hence, use cases I.2.2 and I.1.3 should be identical from ITU-T H.248 control perspective.



I.1.1) Media security "**end-to-access edge**" for application agnostic data traffic, incl. interworking to legacy TCP-based data transport:

I.1.2) Media security "**end-to-end**" for application agnostic data traffic, incl. interworking to legacy TLS/TCP-based data transport:

I.1.3) Media security "**end-to-end**" for application agnostic data traffic in DTLS transparent forwarding mode:

Figure I.1 – Use cases for application protocol agnostic DTLS handling

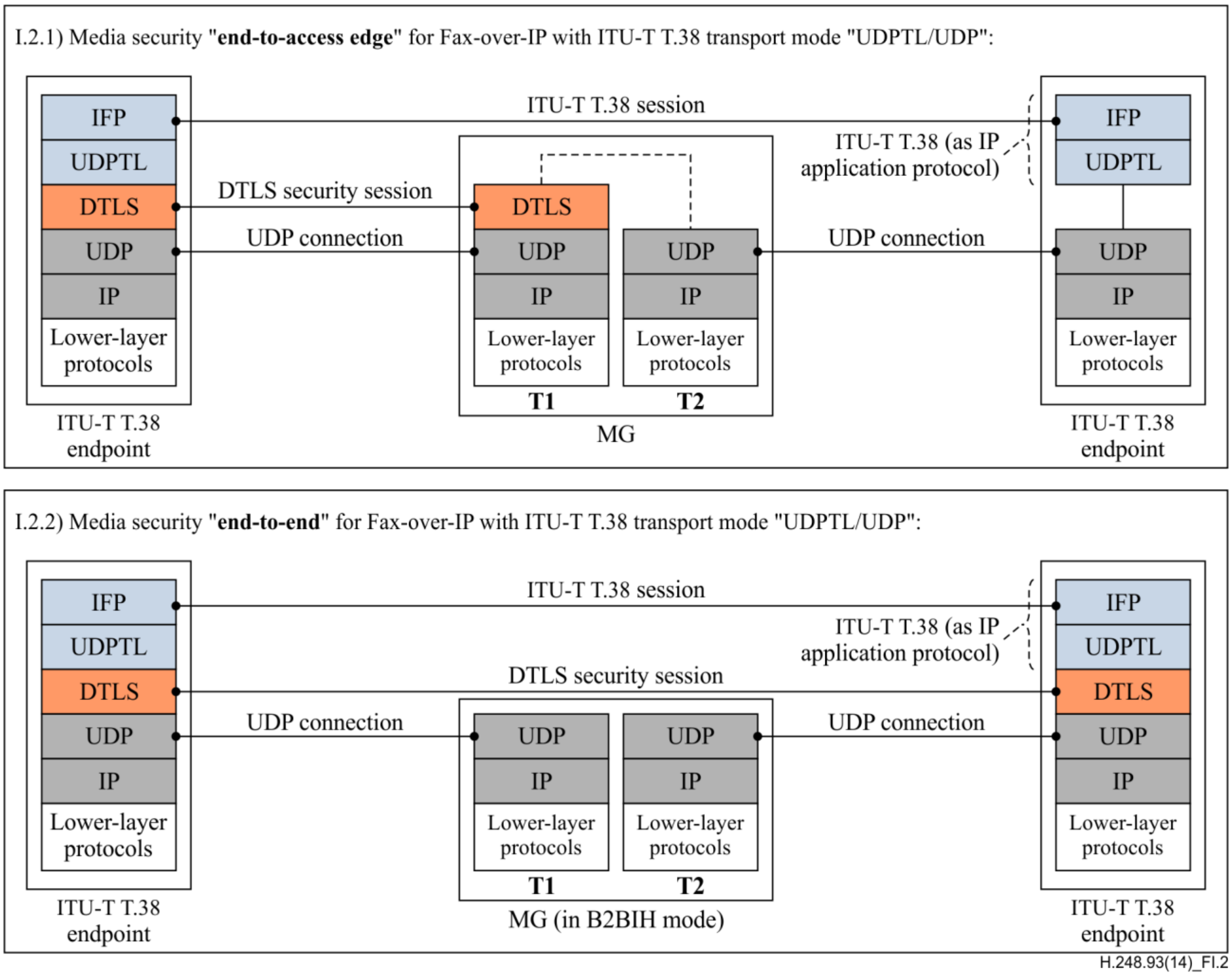


Figure I.2 – Use cases for DTLS-based transport security for ITU-T T.38 fax packet relay service

I.3 Use cases for "WebRTC data traffic"

Background

Web-based real-time communication (WebRTC) relates to a multimedia application inclusive of a data component. The WebRTC data uses a "SCTP/DTLS/UDP" transport.

The WebRTC data traffic related DTLS use cases provide further characteristics in addition to the use cases in clauses I.1 and I.2:

– hierarchical protocol stack layering by using a secured tunnel (given by SCTP/DTLS);

– multiplexing model because a single DTLS security session could be shared by multiple WebRTC data channels; and

– communication between various WebRTC endpoint types leads to UDP-to-UDP and UDP-to-TCP interworking support by ITU-T H.248 MGs.

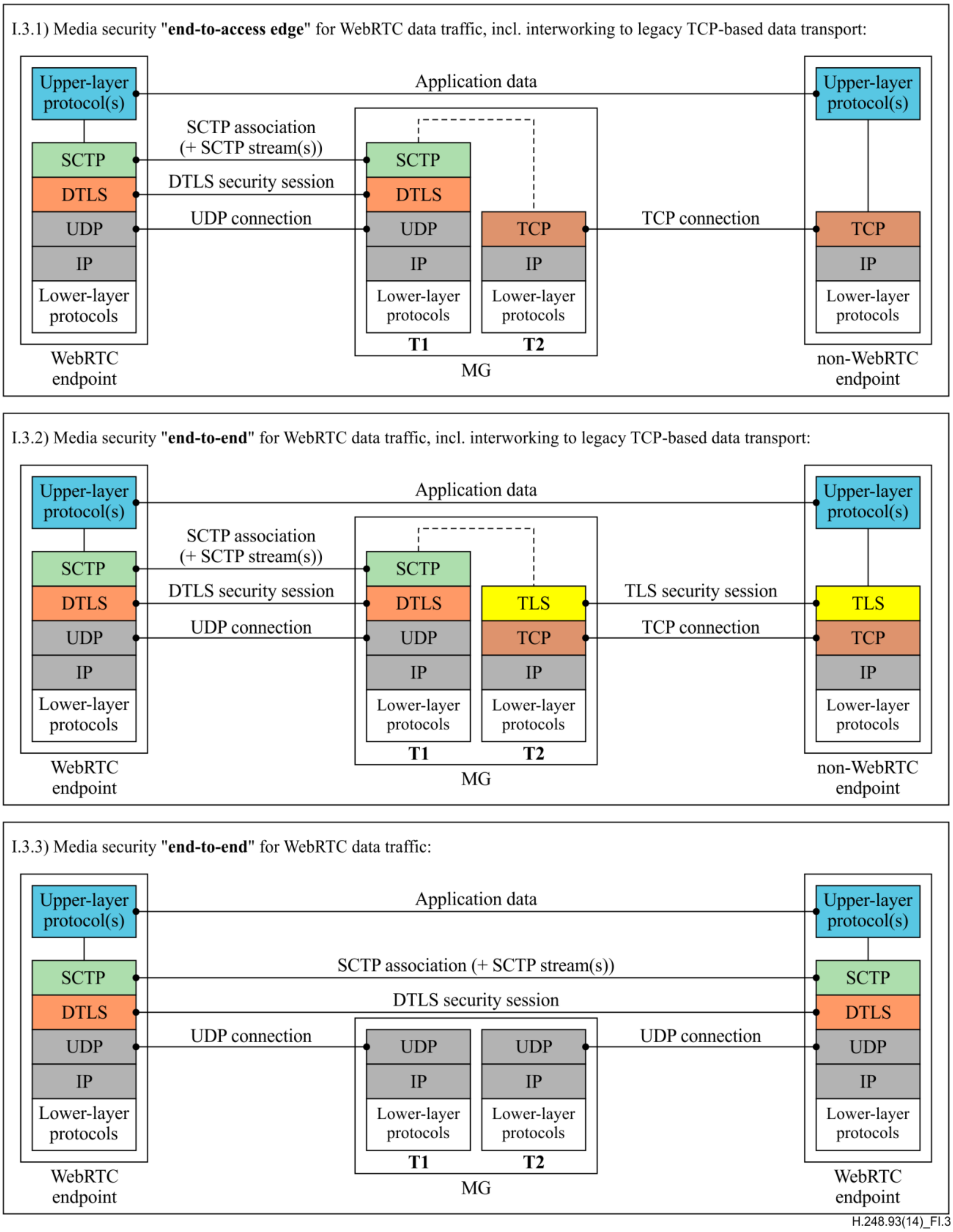
There are three principal use cases in case of end-to-end UDP based transport (see Figure I.3):

– use case I.3.1: MG provides interworking between "SCTP/DTLS/UDP/IP"and "TCP/IP";

– use case I.3.2: MG provides interworking between " SCTP/DTLS/UDP/IP" and "TLS/TCP/IP"; and

– use case I.3.3: MG provides interworking between "(DTLS/)UDP/IP" to "(DTLS/)UDP/IP" in DTLS transparent forwarding mode.

It should be noted that the MG again is not aware of the application protocol itself. However, the main difference is the embedded "SCTP stream/SCTP association" layering in comparison to clause I.1.


I.3.1) Media security "**end-to-access edge**" for WebRTC data traffic, incl. interworking to legacy TCP-based data transport:

I.3.2) Media security "**end-to-end**" for WebRTC data traffic, incl. interworking to legacy TCP-based data transport:

I.3.3) Media security "**end-to-end**" for WebRTC data traffic:

Figure I.3 – Use cases for WebRTC data traffic

I.4 Use cases for "DTLS-based key exchange for SRTP"

There are multiple key exchange options for the secure real-time transport protocol (SRTP), see [b-IETF RFC 7201] and [b-IETF RFC 7202]. One media-path coupled key exchange option is based on DTLS (see clause I.4.1.2).

Another, non-DTLS-based option is already supported by ITU-T H.248. Clause I.4.1.1 summarizes the pure signalling-path coupled key exchange option in order to contrast the DTLS-SRTP variant.

I.4.1 Two considered key exchange options for SRTP

I.4.1.1 Media-path decoupled key exchange using SDP (via SIP and ITU-T H.248)

Figure I.4 illustrates the protocol stack for SDES-based key exchange for SRTP (SDP security descriptions, see [b-IETF RFC 4568]), as in scope of [b-ITU-T H.248.77].

Note that DTLS is not involved.

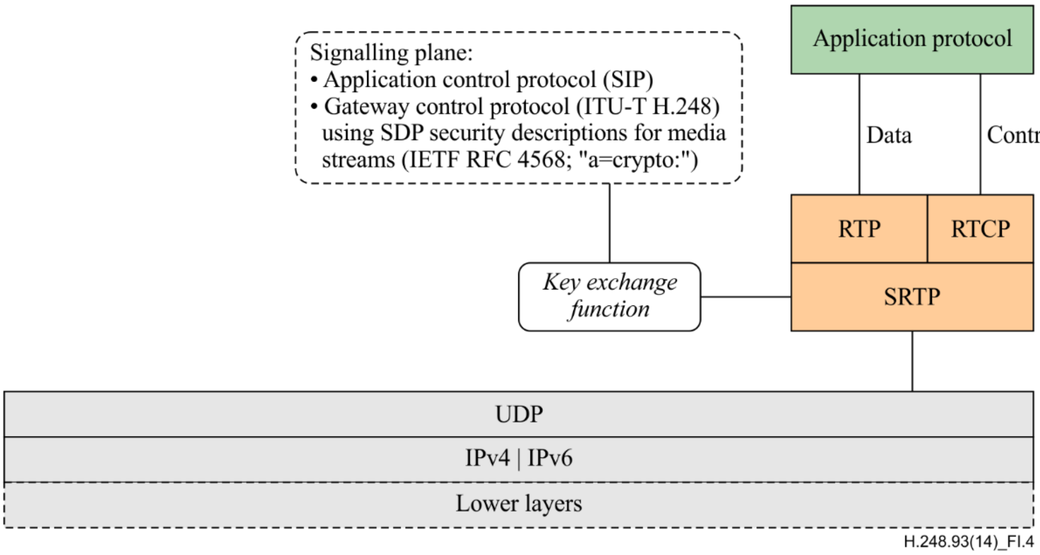

Signalling plane:
• Application control protocol (SIP)
• Gateway control protocol (ITU-T H.248) using SDP security descriptions for media streams (IETF RFC 4568; "a=crypto:")
Application protocol
Data
Control
RTP
RTCP
Key exchange function
SRTP
UDP
IPv4 | IPv6
Lower layers
H.248.93(14)_FI.4

Figure I.4 – Media-path decoupled key exchange using SDP (via SIP and ITU-T H.248)

I.4.1.2 Media-path coupled key exchange using DTLS

Figure I.5 illustrates the alternative of a DTLS-based key exchange for SRTP according to [b-IETF RFC 5763] (framework) and [IETF RFC 5764] (protocol), called briefly "DTLS-SRTP".

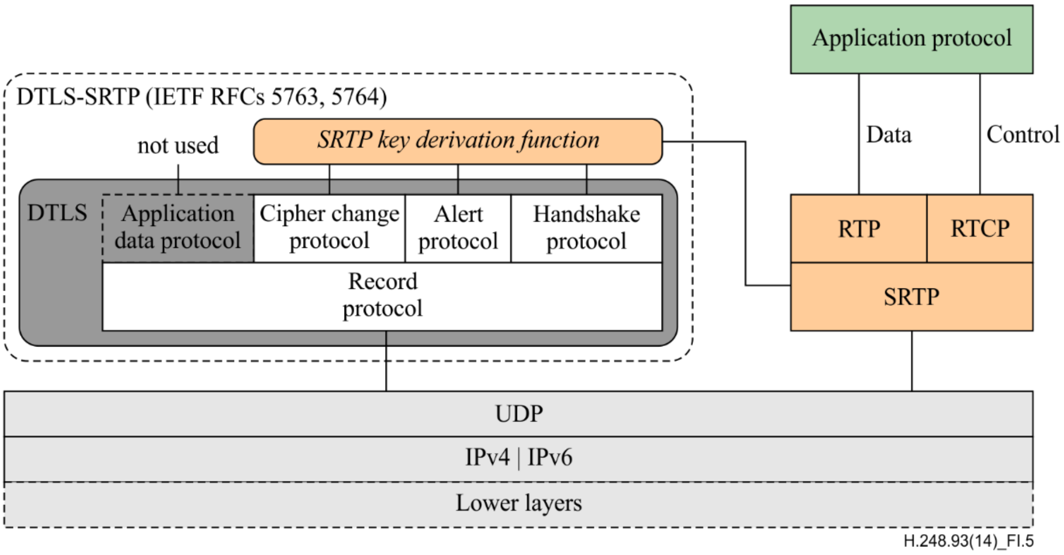


Figure I.5 – Media-path coupled key exchange using DTLS

DTLS-SRTP uses DTLS in a limited way:

- DTLS protocol suite: usage of the DTLS handshake, cipher change and alert protocols (inclusive DTLS record layer), without any application data transfer over DTLS at all; and
- time horizon: only during key derivation, rekeying phases and alert events.

The derivation process of the SRTP keys (using (D)TLS) is detailed in section 4.2 of [IETF RFC 5764].

I.4.2 ITU-T H.248 impact by DTLS-SRTP

DTLS-SRTP introduces some DTLS extensions for SRTP key establishment. The DTLS protocol extension parameters are defined in section 4.1 of [IETF RFC 5764]. These extension parameters are covered by the *dtlscn* package (see clause 11).

Appendix II

Signalling flows for basic DTLS session establishment and release

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

II.1 Overview

The *tlsbsc* package (clause 8 of [ITU-T H.248.90]) defines the basic TLS security session control with scope on support for establishment and release. Basic DTLS session control reuses the solution defined by that package.

II.2 Conventions

An ITU-T H.248 context with a single stream endpoint pair (SEPP); only one SEP (labelled as T1(S1)) is considered. The MG bearer interface (DTLS) is highlighted besides the ITU-T H.248 interface.

Furthermore, all figures indicate possible event notifications to the MGC by the MG. The particular event(s) would be related to state changes of the local DTLS session endpoint.

It has to be noted that some DTLS specifics are not visible at the abstraction level considered, such as:

– Bearer type indication (via SDP "m=" line) when creating a DTLS-enabled SEP/Termination; and

– DTLS timeouts and retransmissions (during e.g., establishment handshake procedures) (i.e., as per Figure 3 "DTLS Timeout and Retransmission State Machine" of [IETF RFC 6347]).

NOTE – IP transport protocol: L4 bearer connection control procedures are optional, dependent on a connection-oriented IP transport protocol (see clause 6.1). Such procedures are indicated, but out of scope of this appendix.

II.3 Establishment of DTLS security sessions

II.3.1 Successful establishment, terminating side

See Figure II.1, termed as use case (E.1).

More details for this example:

– The MGC blocks the start of DTLS session establishment (1).

– Early incoming DTLS messages are discarded by the MG (2).

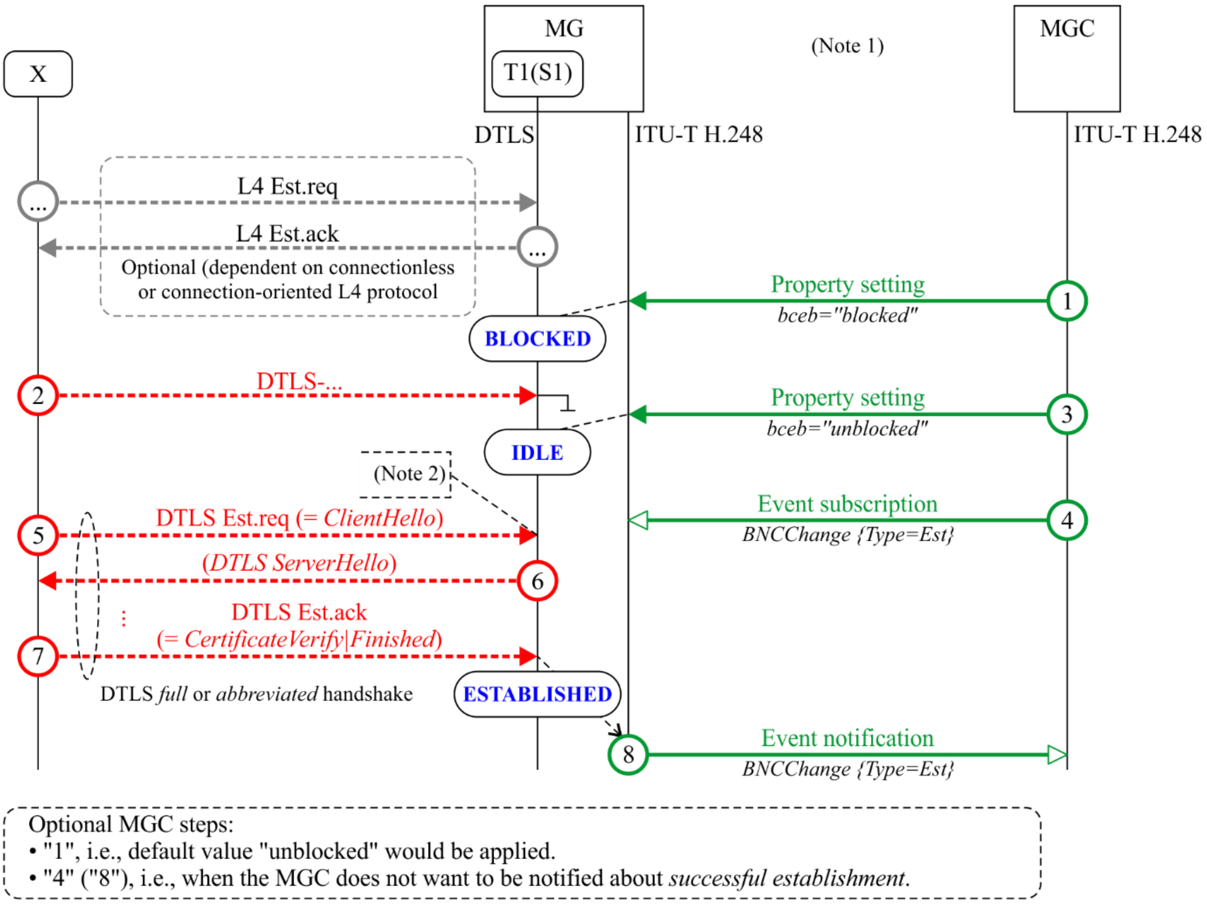
– The MGC unblocks the DTLS SEP (3).

– DTLS session establishment (5 to 7); MG acting as DTLS server.

– Optional notification of MGC concerning available DTLS session for application data transfer (8), if subscription to event by MGC (4).

II.3.2 Successful establishment, originating side

See Figure II.2, use case (E.2).



NOTE 1 – Abstracted ITU-T H.248 commands, also replies are not shown.

NOTE 2 – Implies "DTLS server" role assignment to SEP T1(S1).

Figure II.1 – Successful establishment, terminating side

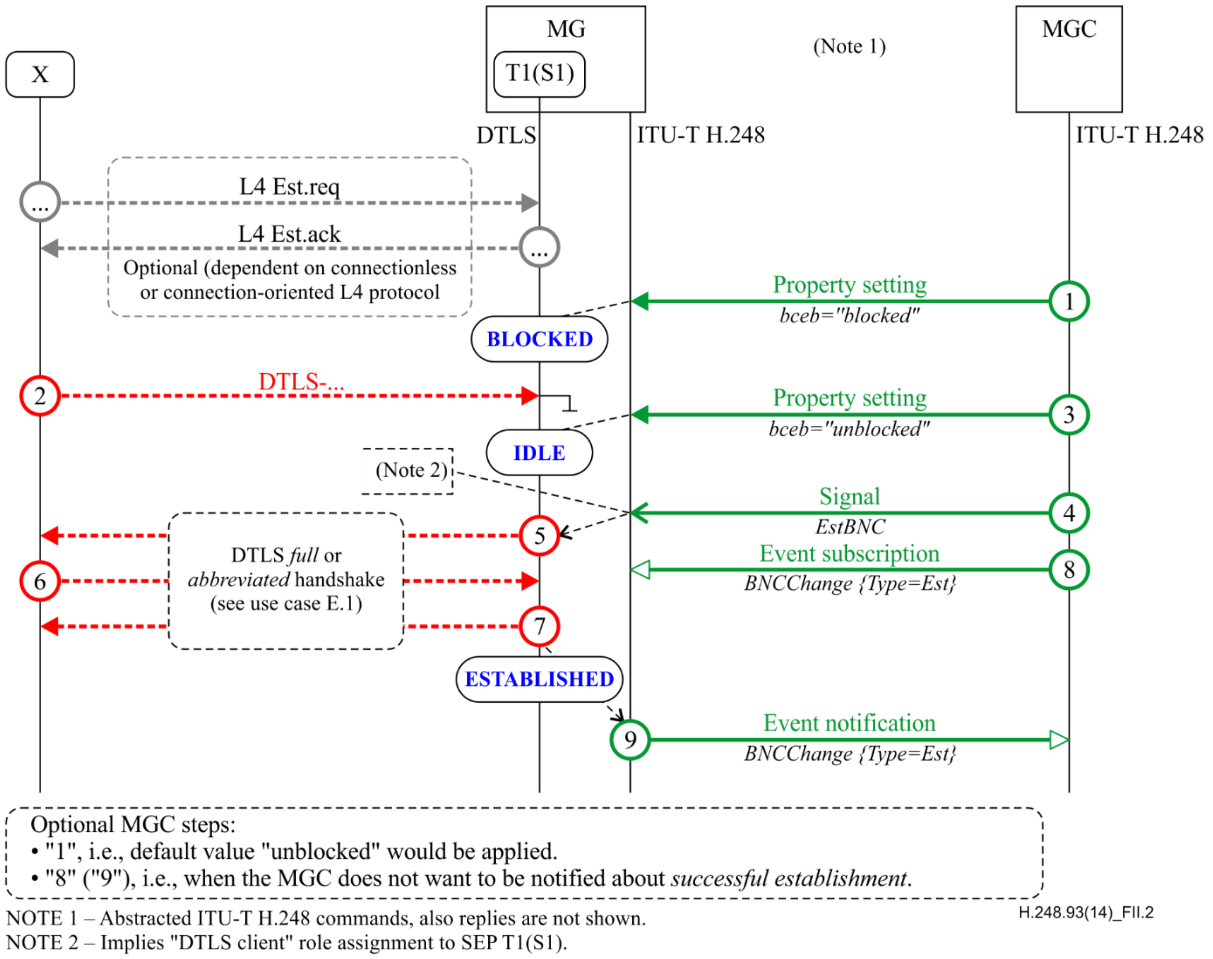

MG
T1(S1)
MGC
(Note 1)
X
DTLS
ITU-T H.248
ITU-T H.248
L4 Est.req
L4 Est.ack
Optional (dependent on connectionless or connection-oriented L4 protocol
Property setting
bceb="blocked"
1
BLOCKED
2
DTLS-...
Property setting
bceb="unblocked"
3
IDLE
(Note 2)
Signal
EstBNC
4
5
Event subscription
BNCChange {Type=Est}
8
6
DTLS full or abbreviated handshake (see use case E.1)
7
ESTABLISHED
9
Event notification
BNCChange {Type=Est}
Optional MGC steps:
• "1", i.e., default value "unblocked" would be applied.
• "8" ("9"), i.e., when the MGC does not want to be notified about successful establishment.
NOTE 1 – Abstracted ITU-T H.248 commands, also replies are not shown.
NOTE 2 – Implies "DTLS client" role assignment to SEP T1(S1).
H.248.93(14)_FII.2

Figure II.2 – Successful establishment, originating side

More details for this example:

- Steps 1 to 3 as in clause II.3.1
- DTLS session establishment (5 to 7), triggered by MGC (4); MG acting as DTLS client.
- Optional notification of MGC concerning available DTLS session for application data transfer (9), if subscription to event by MGC (8).

II.3.3 Unsuccessful establishment

The DTLS security session negotiation handshake is not completed.

II.4 Release of DTLS security sessions

II.4.1 Successful release – Terminating side

See Figure II.3, termed as use case (R.1).

More details for this example:

- MG receives an incoming DTLS close_notify alert (2), the indication for DTLS session release.
- The MG acknowledges the release request (3).
- Optional notification of MGC concerning successfully released DTLS session (4), if subscription to event by MGC (1).

II.4.2 Successful release – Originating side

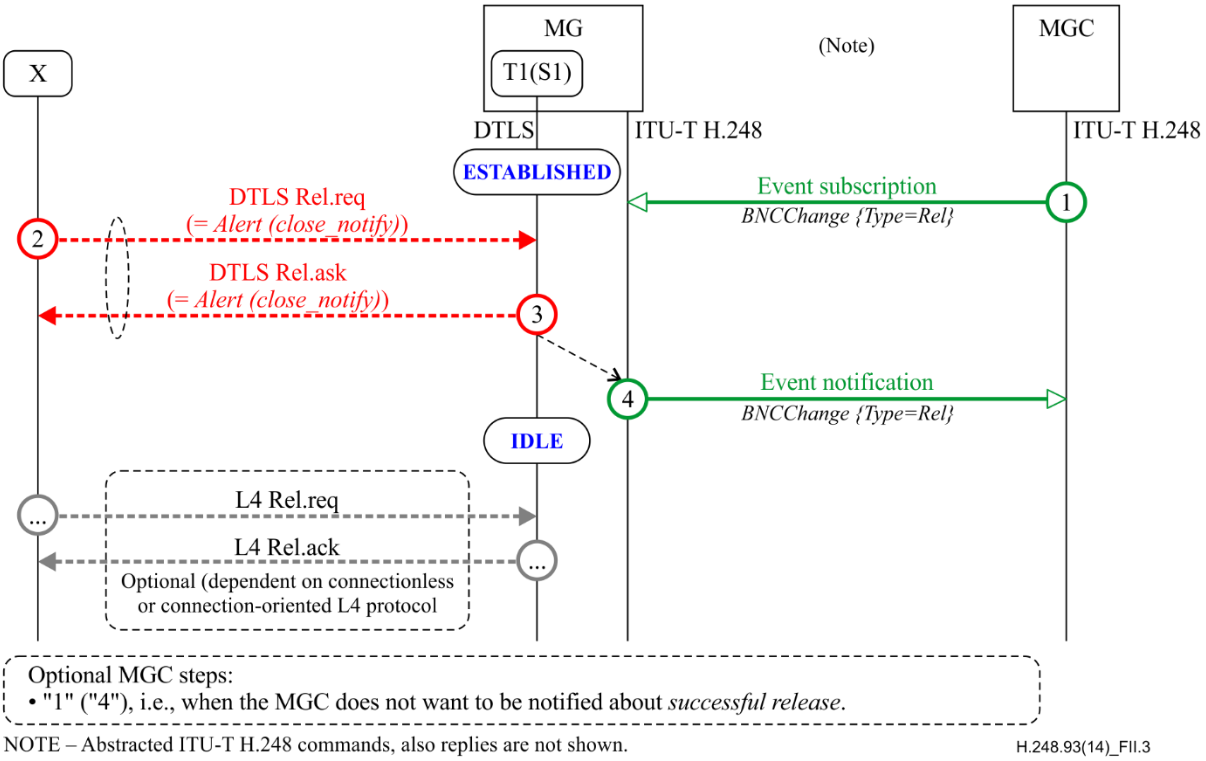
See Figure II.4, use cases (R.2) illustrates an outgoing DTLS session release.

More details for this example:

- MGC initiates the DTLS session release (1).
- MG sends an outgoing DTLS close_notify alert (2), the indication for DTLS session release towards remote DTLS endpoint X.
- Successful release (3).
- Optional notification of MGC concerning successfully released DTLS session (5), if subscription to event by MGC (4).

II.4.3 Unsuccessful release

An unsuccessful DTLS session release procedure would imply that the MG remains in ITU-T H.248 state Established and that the MGC could possibly suspect a still established DTLS session. There are multiple options on how such protocol deadlocks could be resolved. For example, the situation could be cleared by the subtraction of the termination by the MGC.



NOTE – Abstracted ITU-T H.248 commands, also replies are not shown.

Figure II.3 – Successful release, terminating side

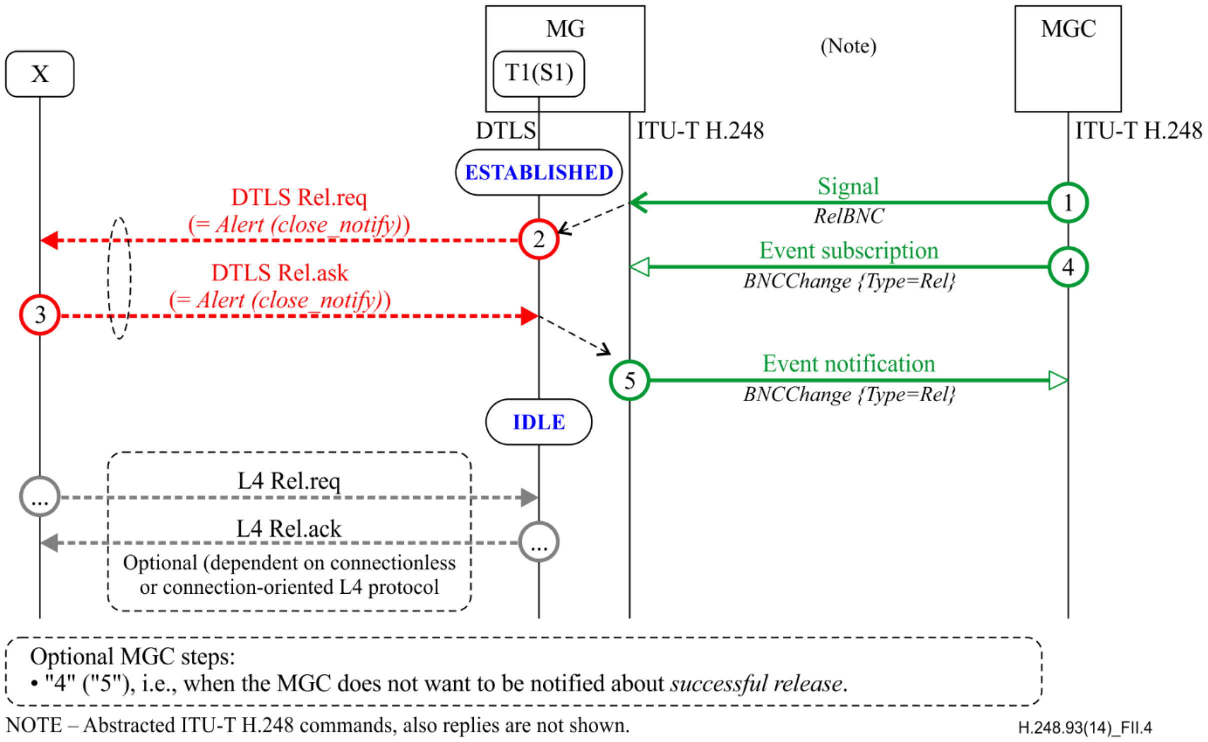


Figure II.4 – Successful release, originating side

Bibliography

[b-ITU-T H.248.77] Recommendation ITU-T H.248.77 (2010), *Gateway control protocol: Secure real-time transport protocol (SRTP) package and procedures*.

[b-ITU-T T.38] Recommendation ITU-T T.38 (2010), *Procedures for real-time Group 3 facsimile communication over IP networks*, including its Amendment 1 (2014).

[b-ITU-T V.153] Recommendation ITU-T V.153 (2009), *Interworking between ITU-T T.38 and ITU-T V.152 using IP peering for real-time facsimile services*.

[b-IETF RFC 4347] IETF RFC 4347 (2006), *Datagram Transport Layer Security*.

[b-IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams*.

[b-IETF RFC 5238] IETF RFC 5238 (2008), *Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP).*

[b-IETF RFC 5763] IETF RFC 5763 (2010), *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*.

[b-IETF RFC 6083] IETF RFC 6083 (2011), *Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP).*

[b-IETF RFC 7201] IETF RFC 7201 (2014), *Options for Securing RTP Sessions*.

[b-IETF RFC 7202] IETF RFC 7202 (2014), *Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security Solution*.

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, 2015