International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.91

(10/2014)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

---

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

Recommendation ITU-T H.248.91

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.248.91

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

Summary

Recommendation ITU-T H.248.91 provides guidelines on the use of secured IP bearer traffic according to the transport layer security (TLS) technology in ITU-T H.248 profiles. These guidelines may be used by other standards developing organizations (SDOs) when defining their ITU-T H.248.1 profiles in support of TLS.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.248.91	2014-10-14	16	11.1002/1000/12242

* 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

Recommendation ITU-T H.248.91

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

1 Scope

Transport layer security (TLS) is a cryptographic protocol that provides secure communication between two IP transport endpoints. This Recommendation:

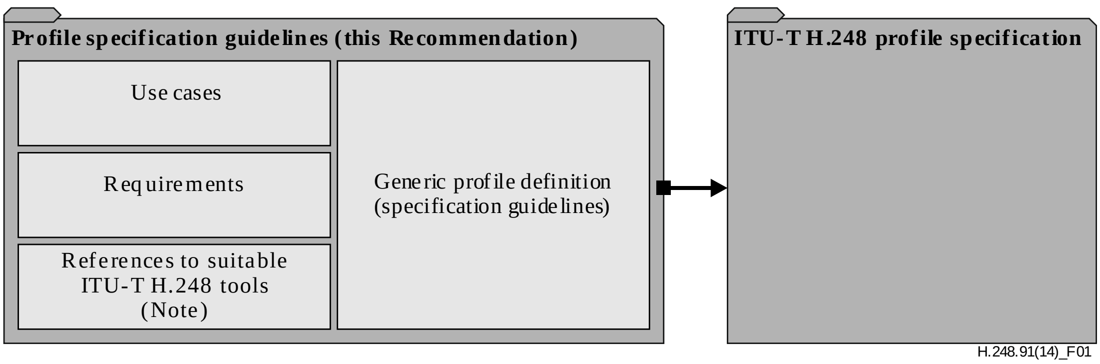
– describes example use cases;

– defines the basic requirements to secure the bearer path connection between a media gateway (MG) and a remote endpoint through TLS;

– references suitable ITU-T H.248 signalling capabilities in terms of ITU-T H.248 packages as defined by other ITU-T H.248.x-series Recommendations; and

– defines a protocol solution in style of a generic profile (which covers usage information of package(s) and procedures) as a guideline for final profile specifications.

The scope and purpose of this Recommendation is illustrated in Figure 1:



NOTE – E.g., ITU-T H.248 packages according to [ITU-T H.248.84], [ITU-T H.248.89], [ITU-T H.248.90], etc.

Figure 1 – Scope, structuring principle and framework of this Recommendation

The primary audience of this Recommendation are therefore authors of ITU-T H.248 profile specifications, which aim to support a particular network use case with TLS encrypted bearer traffic (based on the example *use cases* from Appendix II of [ITU-T H.248.90]).This Recommendation is organized as follows:

– examples;

– principal *requirements* are subject of clauses 6 to 9, categorized in capabilities with regards to the mode of operation of a MG, TLS profile concepts and TLS protocol specific requirements;

and

– profile specification guidelines in clause 10 (which follows the profile structure of the ITU-T H.248 profile template according to [ITU-T H.248.1]).

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.248.84] Recommendation ITU-T H.248.84 (2012), *Gateway control protocol: NAT traversal for peer-to-peer services*.

[ITU-T H.248.89] Recommendation ITU-T H.248.89 (2014), *Gateway control protocol: TCP support packages*.

[ITU-T H.248.90] Recommendation ITU-T H.248.90 (2014), *Gateway control protocol: ITU-T H.248 packages for control of transport security using transport layer security (TLS)*.

[ITU-T X.509] Recommendation ITU-T X.509 (2012), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.

[IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program – Protocol Specification*.

[IETF RFC 2712] IETF RFC 2712 (1999), *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*.

[IETF RFC 3436] IETF RFC 3436 (12/2002), *Transport layer security over stream control transmission protocol*.

[IETF RFC 4120] IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*.

[IETF RFC 4145] IETF RFC 4145 (2005), *TCP-Based Media Transport in the Session Description Protocol (SDP)*.

[IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

[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 4583] IETF RFC 4583 (2006), *Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

See TLS related terminology in [ITU-T H.248.90].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AN	Access Network
API	Application Program Interface
BFCP	Binary Floor Control Protocol
CA	Certification Authority
CN	Core Network
CS	Capability Set
DB	Data Base
e2ae	End-to-Access-Edge (security model)
IP	Internet Protocol
IWF	Interworking Function
Lx	Layer number
MG	Media Gateway
MGC	Media Gateway Controller
NAPT	Network Address and Port Translation
PSK	Pre-Shared Key
SCTP	Stream Control Transmission Protocol
SDO	Standards Developing Organization
SDP	Session Description Protocol
SEP	Stream Endpoint
SHA	Secure Hash Algorithm
TCP	Transport Control Protocol
TLS	Transport Layer Security
UE	User Equipment

5 Conventions

This Recommendation provides a list of items, labelled as ***R-x/y***, where *x* refers to the clause number and *y* a number within that clause. Such items use the following keywords with meanings as prescribed below:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the Recommendation.

6 Requirements for control the MG mode of operation

6.1 TLS transport mode

TLS is designed as a transport-independent protocol, just making the assumption of "reliable transport" of the underlying protocol (see section 1 of [IETF RFC 5246]). Support of one or multiple TLS transport mode(s) is required.

R-6.1/1: Transport mode "TLS-over-TCP".

NOTE – This requirement would be applicable for the very majority of use cases.

R-6.1/2: Transport mode "TLS-over-SCTP" [IETF RFC 3436].

It may be noted that TLS protocol procedures need to be decoupled from protocol procedures of the underlying transport protocol.

6.2 MG mode of operation for case of TLS-over-TCP transport

A particular mode of operation (of the MG) is given by:

– ITU-T H.248 SEP view: given by a particular configuration of the TLS/TCP/IP protocol stack (e.g., TCP client, TLS server, etc.);

– ITU-T H.248 Context view: given by the connection model, typically by two associated stream endpoints (SEPs) (e.g., TCP proxy or relay mode).

See also clause 13.5 "Indication of 'TCP mode' for ITU-T H.248 MG" in [ITU-T H.248.84].

R-6.2/1: The media gateway controller (MGC) is required to control the TCP/TLS specific characteristics of the ITU-T H.248 stream. This comprises:

– the mode of operation in the MG, TCP-proxy vs. TCP-relay;

– the TCP-connection mode for each TCP-SEP of the ITU-T H.248 Context (TCP-server vs. TCP-client); and

– the TLS-connection mode for each TCP/TLS-SEP of the ITU-T H.248 Context (TLS-server vs. TLS-client).

NOTE – The TLS-connection mode of a SEP may be set independently of its related TCP-connection mode.

R-6.2/2: The TCP-mode of operation to be applied between two SEPs within a MG depends on the processing of the TCP-byte-stream within the MG. In case an entity located above the TCP-layer within the MG is TCP-payload aware, the TCP-layer is required to deliver the byte stream in a reliable and ordered manner to that entity.

R-6.2/3: Thus, the presence of at least one TLS entity is a sufficient condition to require the TCP-proxy mode. Refer to Figure 2.

NOTE 1 – There might be multiple entities present which require the TCP-proxy mode, e.g., in case both terminations of a Context are TLS-enabled, or if another application-aware interworking function is performed by the MG.

NOTE 2 – The term "application" is widely used in TCP-related Contexts, but in this Recommendation it is used as a synonym for the term "media".

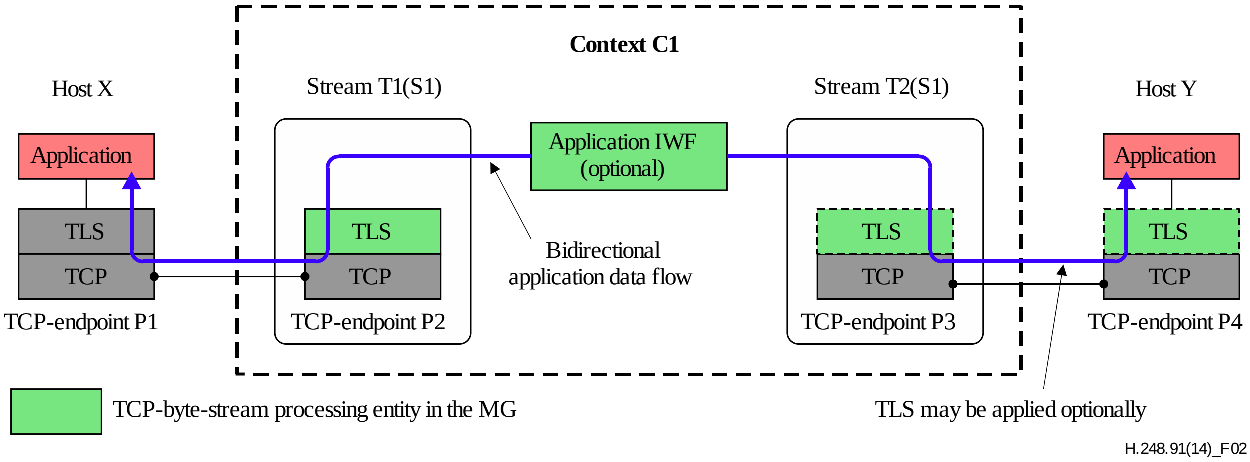


Figure 2 – TCP-byte stream processing entities located in the MG

Although the requirement above seems to require a "full TCP-proxy" mode for the entire lifetime of the TCP-session, there might be use cases for which at least for a dedicated period of the session a simplified TCP-proxy mode makes sense, e.g., from system resource perspective. Such a "lightweight TCP-proxy" mode is for further study.

Besides the termination of a TLS session, the MG may be required to perform an application data interworking function. Thus, the MG may operate in an "application agnostic TCP-proxy" mode as depicted in Figure 3, or as an "application aware TCP-proxy as shown in Figure 4.

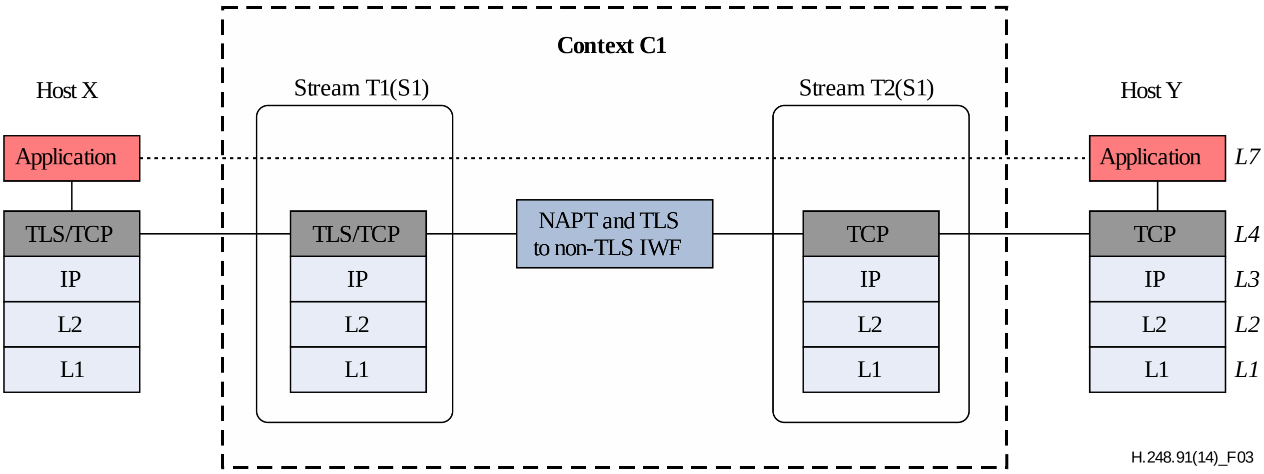


Figure 3 – "Application agnostic" TCP-proxy with TLS to non-TLS interworking

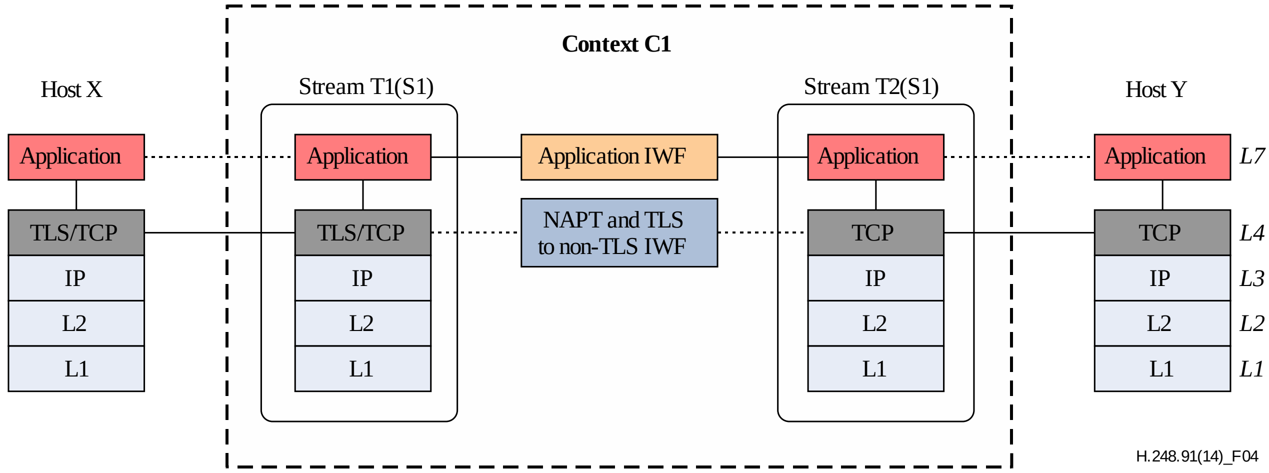


Figure 4 – "Application aware" TCP-proxy with TLS to non-TLS interworking

The indication of the TCP-proxy mode is defined by [ITU-T H.248.84]; the procedures to control a SEP in the TCP proxy modes are extended by [ITU-T H.248.89].

R-6.2/4: The MGC shall have the capability to control the set-up of the TCP-connection.

R-6.2/5: The MG is required to conform to the TCP protocol according to [IETF RFC 793].

7 Requirements given by a TLS Profile concept

"*The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery*." [IETF RFC 5246]

Besides the basic TLS standard, a set of TLS extensions has been defined as well which provides several optional features for a TLS implementation to choose from. A TLS profile defines a specific set of those features to reduce interoperability issues for a TLS session between two endpoints following the same TLS profile.

7.1 Requirements to such a TLS profile

R-7.1/1: The MG's implementation is required to comply with the TLS profile of the selected TLS domain (see clause 8.1) (also called *TLS domain profile*; see terminology in [ITU-T H.248.90]).

NOTE – The remote TLS endpoint should comply to the same TLS profile as well, but this is out of scope of this Recommendation.

7.2 Requirements to elements of TLS profiles

R-7.2/1: The MG is required to support the TLS version(s) as specified by the TLS profile.

NOTE – The following TLS versions have been published: TLS version 1.1 [b-IETF RFC 2246], TLS version 1.2 [b-IETF RFC 4346] and [IETF RFC 5246]. The TLS version 1.3 is currently under development in IETF.

R-7.2/2: The MG is required to support the cipher suites as specified by the TLS profile. The precedence of cipher suites, as defined by the profile, is required to be taken into account.

R-7.2/3: The MG is required to support the compression method as specified by the TLS profile.

R-7.2/4: The MG is required to support the renegotiations of the security parameters for an existing TLS session. The renegotiation behaviour may be defined by the TLS profile or may be provided by the MGC prior to the actual bearer path coupled TLS session renegotiation.

NOTE – There is the assumption that the MGC will not be actively involved in the renegotiation procedure.

R-7.2/5: The MG is required to support the session resume as specified by the IETF TLS related RFCs.

R-7.2/6: The MG is required to support the authentication procedures as specified by the TLS profile.

R-7.2/7: In case the MG is required to verify a signed certificated received from the remote TLS endpoint, the MG is required to use the list of root certificates associated with the TLS profile.

NOTE – The "root certificate" concept might be replaced by "trust anchor" information (see [b-IETF RFC 5914] and [ITU-T X.509]) in a future edition of this Recommendation.

8 Requirements on TLS procedures

8.1 Selection of the TLS domain

A MG may be connected to multiple network domains with different TLS profiles. Figure 5 illustrates such a use case[1] (with scope on TCP bearer traffic) using the example of an ITU-T H.248 IP-IP MG located at the edge between the access network (AN) and the core network (CN) domains. The CN belongs to a trusted domain, hence transports unencrypted TCP traffic. Multiple different, TLS-enabled AN domains may be the result of multiple different access technologies, trust models, service provider models, etc.

[1] This use case is a variation of use case #1.4 from clause 6.2.1 of [ITU-T H.248.90].

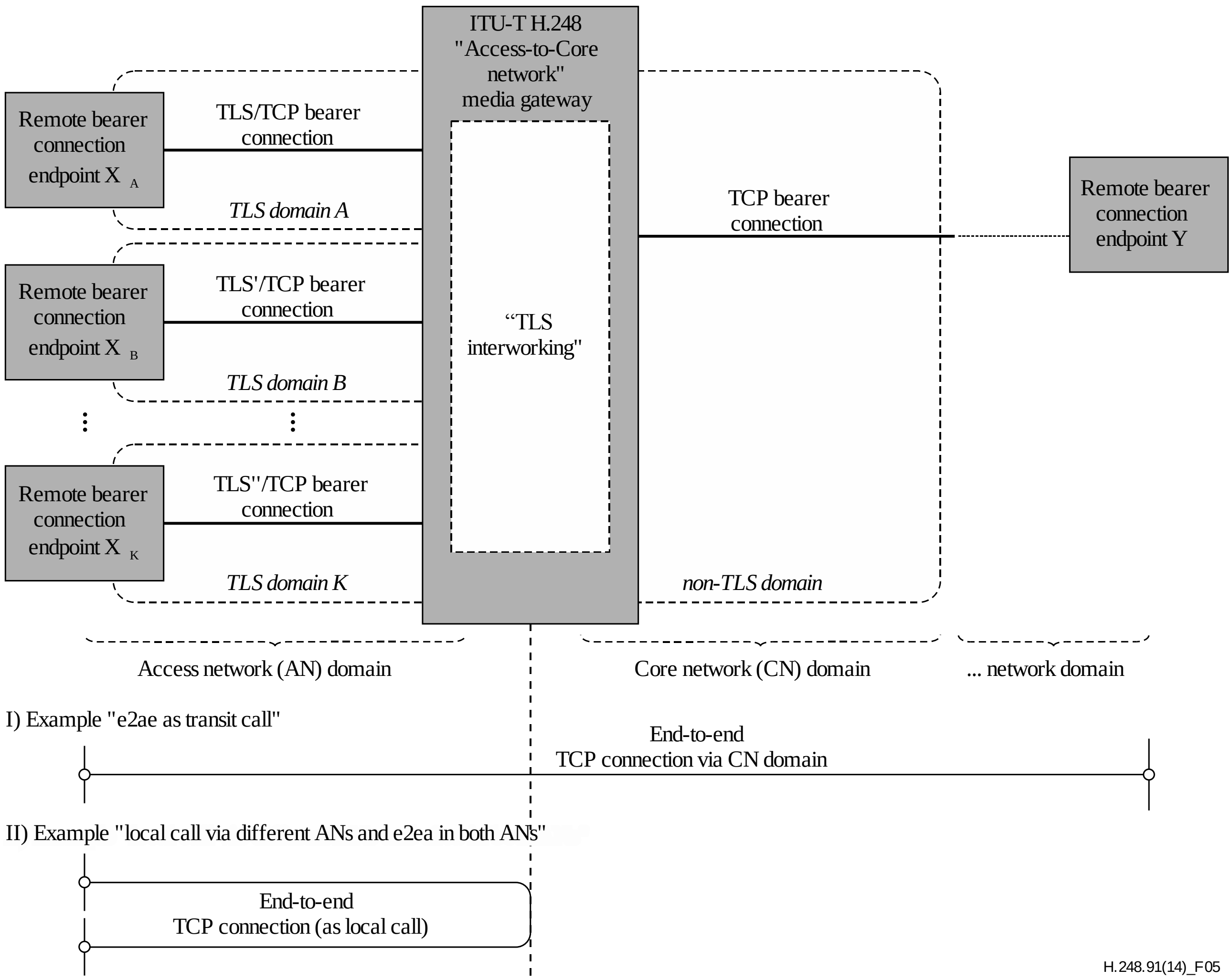


Figure 5 – Use case: MG connected to multiple, different TLS domains

It should be noted that there could be, but there must not be necessarily, a one-to-one relationship between an "IP address realm" [b-ITU-T H.248.37] and a "TLS domain". For instance, a particular access network domain may support IPv4 and IPv6 terminals, but represent just a single TLS domain ("same TLS security support, independent from IP version").

R-8.1/1: The MGC is required to provide the TLS domain towards the MG upon creation of a TLS endpoint, under the condition of multiple TLS domains connected to the MG.

R-8.1/2: The MGC is not required to provide TLS domain related information to the MG, under the condition that just a single TLS domain is served.

R-8.1/3: The MG is required to apply the TLS profile based on the provided TLS domain for the created TLS endpoint.

R-8.1/4: The MG is required to use the certificate for authentication that is associated with the provided TLS domain, if certificate based authentication is applicable.

8.2 Client/Server Mode

8.2.1 TLS client/server role assignments

R-8.2.1/1: The MG is required to support both the TLS server and TLS client modes.

The TLS standards do not make any correlation between the initiation of the underlying transport connection and the TLS client/server mode. Thus, this mode is decoupled from the (TCP) SDP "a=setup:" attribute (as introduced by [IETF RFC 4145]), as used for TLS-based SDP indications (see clause 4 of [IETF RFC 4572]).

R-8.2.1/2: The MGC is required to indicate the TLS server/client role to the MG.

NOTE – There is no existing TLS related session description protocol (SDP) defined which represents TLS client/server semantic. [IETF RFC 4572] intentionally delegates such control information to the application (layer).

R-8.2.1/3: The MG is required to select the TLS client or TLS server role based on the MGC request.

8.2.2 Client/server role assignments to TLS transport protocols

R-8.2.2/1: Any IP transport protocol level client/server role assignment shall be independent of TLS server and TLS client mode.

Justification:

– TLS is principally designed to be independent from IP transport protocols [IETF RFC 5246], in order to support multiple transport options (e.g., TCP, SCTP).

– Stream control transmission protocol (SCTP) (as TLS transport candidate) does not provide a client/server concept.

– Application protocol binary floor control protocol (BFCP): TCP client/server roles are decoupled from TLS client/server roles (in case of BFCP-over-TLS/TCP), see [IETF RFC 4583].

8.3 Behavioural requirements for authentication

The TLS protocol has been extended by several IETF RFCs and provides several mechanisms for client/server authentication. Client and server authentication can be optional, but normally at least one of the TLS endpoints is authenticated. The TLS-server controls whether the TLS-client is authenticated.

For a TLS session, the methods used for server authentication may differ from the method used for client authentication.

8.3.1 General

R-8.3.1/1: The TLS profile is required to specify whether the client or server authentication is required.

R-8.3.1/2: The TLS profile is required to define the behaviour of the MG in case an authentication fails. Usually a failed authentication leads to the termination of the TLS session, but use cases may exist where the continuation of the TLS session is acceptable (e.g., expired certificates).

R-8.3.1/3: The TLS profile is required to define the conditions when a failed authentication is required to lead to the continuation of the session.

R-8.3.1/4: The authentication methods to be supported by the MG are required to be defined by the TLS profile.

The requirements for the different authentication methods are collected in this clause.

8.3.2 No authentication

R-8.3.2/1: In case the TLS profile defines a cipher suite where the authentication of a TLS-client is optional, the TLS profile is required to define which option the TLS-server shall choose. Possible options are:

– Server is required not to authenticate the client.

– Server is required to authenticate the client.

8.3.3 Authentication through certificates

R-8.3.3/1: The MG is required to support self-signed X.509 certificates (see [ITU-T X.509]) for the MG's certificate.

R-8.3.3/2: The MG is required to support self-signed X.509 certificates (see [ITU-T X.509]) for certificates received from the remote TLS endpoint.

R-8.3.3/3: The MG is required to support CA-signed X.509 certificates (see [ITU-T X.509]) for the MG's certificate.

R-8.3.3/4: The MG is required to support CA-signed X.509 certificates (see [ITU-T X.509]) for certificates received from the remote TLS endpoint.

R-8.3.3/5: The MG is required to support multiple certificates, one per TLS domain.

R-8.3.3/6: The MG is required to select its certificate used for authentication based on the TLS profile that applies for the TLS session.

8.3.3.1 Certificates issued by CAs

NOTE – Certificates that have been issued and signed by a certification authority (CA) are called "signed certificates". An identity certificate signed by the same entity whose identity it certifies is called "self-signed certificate".

R-8.3.3.1/1: When receiving a signed certificate from the remote TLS endpoint, the MG is required to verify the certificate.

R-8.3.3.1/2: In case the signed certificate verification fails, the MG is required to regard the remote TLS endpoint as not authenticated. The behaviour in such a case is required to be defined by the TLS profile, refer to clause 8.3.1, requirements R-8.3.1/2 and R-8.3.1/3.

8.3.3.2 Self-signed certificates

Self-signed certificates used for authentication can be protected against tampering by using fingerprints of the certificate. Those fingerprints consist of a hash algorithm (e.g., SHA-1) and the corresponding hash value of the certificate.

8.3.3.2.1 Applicability requirements

Self-signed certificates can be transported in a signalling information element over the IP signalling paths (see Figure 6). As long as the integrity on the signalling information is assured, the certificate of the remote TLS endpoint can be verified against the fingerprint. How this information element is defined on the signalling path between the MGC and the remote endpoint, and how the integrity of that information element is assured (not only between the MGC and the endpoint but also on the ITU-T H.248 interface) is out of scope of this Recommendation. For further reference, see [IETF RFC 4572].

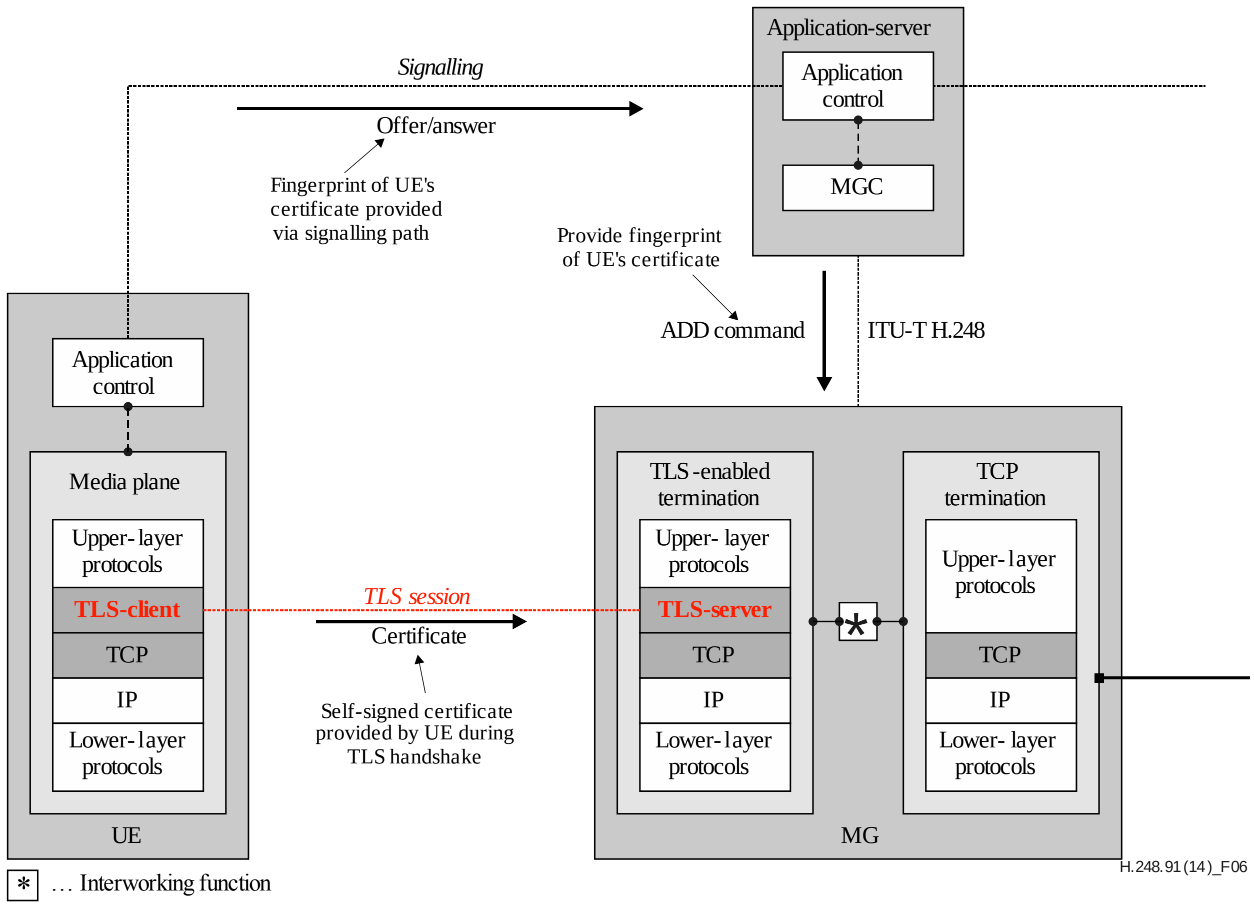


Figure 6 – Use case: Fingerprint of the self-signed certificate passed via signalling path to MG

R-8.3.3.2.1/1: It is prohibited to use self-signed certificates when transport integrity cannot be guaranteed.

R-8.3.3.2.1/2: Self-signed certificates can optionally be used at the ITU-T H.248 interface when the integrity of the ITU-T H.248 Control Association can be assured.

NOTE – This requirement is derived from "TLS-based SDP" usage from application control signalling, following the discussion and explanation of section 3.3 of [IETF RFC 4572].

8.3.3.2.2 Verifying the remote endpoint's self-signed certificate

R-8.3.3.2.2/1: In case the fingerprint information from the remote TLS endpoint is received on the signalling path, the MGC is required to pass this information to the MG.

R-8.3.3.2.2/2: In case the fingerprint information is received by the MG, the MG is required to verify the received self-signed certificate from the remote TLS endpoint against the fingerprint.

R-8.3.3.2.2/3: In case the verification fails, or in case the fingerprint information element has not been received by the MG, the MG is required to regard the remote TLS endpoint as not authenticated.

8.3.3.2.3 Self-signed certificate usage for own TLS endpoint authentication

R-8.3.3.2.3/1: In case the local TLS endpoint is to be authenticated by a self-signed certificate, the MG is required to include the fingerprint information of the certificate in the command reply that is generated as a response of the TLS endpoint creation.

R-8.3.3.2.3/2: The hash algorithm used to generate the fingerprint in the MG is required to be defined by the TLS profile.

R-8.3.3.2.3/3: The MGC is required to include the fingerprint received in the ITU-T H.248 command reply from the MG into the appropriate information element on the signalling path.

8.3.4 Pre-shared keys

Pre-shared keys (PSKs) are symmetric keys shared in advance between the two TLS endpoints. Figure 7 provides an overview of the generic ITU-T H.248 model for a pre-shared key configuration:

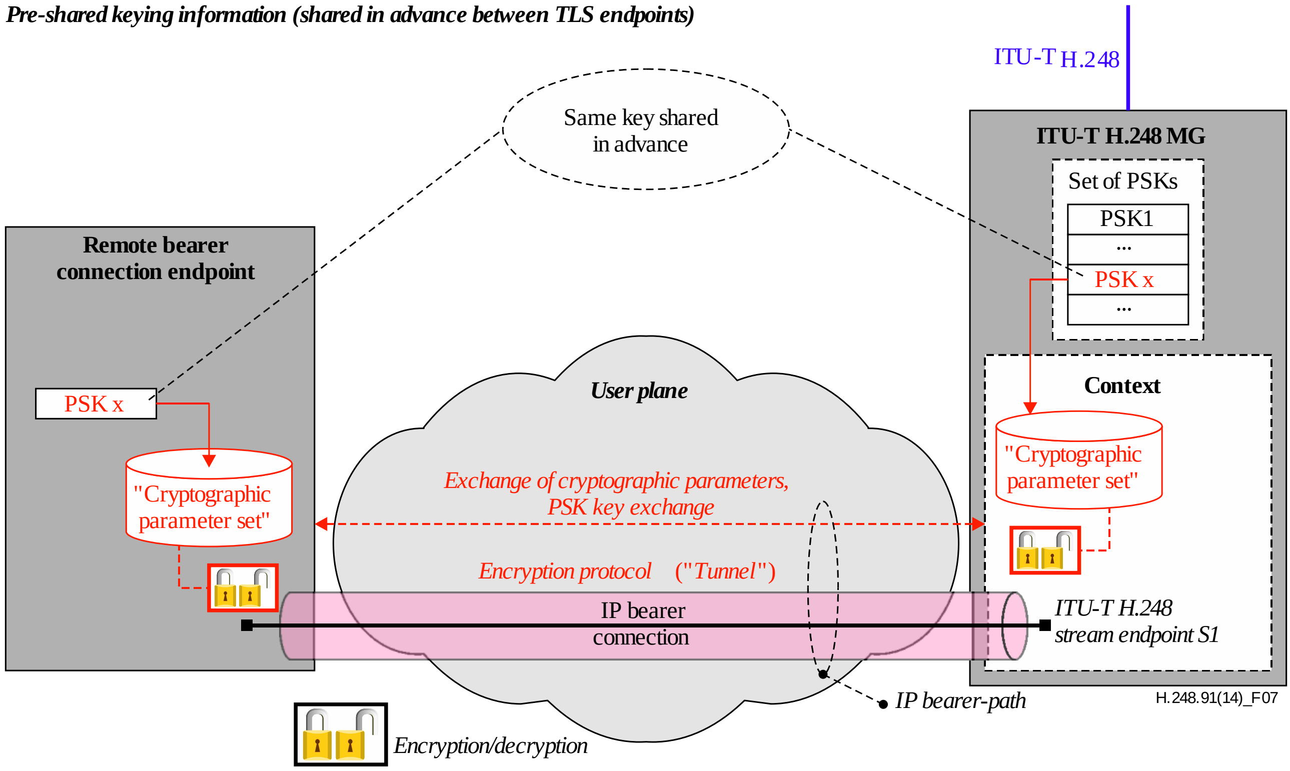


Figure 7 – Generic ITU-T H.248 model for pre-shared keying information

TLS profiles may define one or more PSK cipher suites. To support such cipher suites, the following requirements apply:

R-8.3.4/1: The MG's implementation of the PSK cipher suites is required to be conformant to [IETF RFC 4279].

R-8.3.4/2: The MG is required to support multiple PSKs.

R-8.3.4/3: If acting in the TLS-client mode, the MG is required to select the PSK based on information received from the MGC.

R-8.3.4/4: The MGC is required to indicate the pre-shared key identity to be used for this TLS endpoint towards the MG.

R-8.3.4/5: In case the TLS endpoint to be created is required to act as a TLS-server, the MGC can optionally provide an indication via ITU-T H.248 that indicates the PSK identity hint towards the MG.

8.3.5 Trusted third-party server

A third-party server located in the same TLS-domain and trusted by both TLS endpoints can be used to exchange keying information (Figure 8). For example, the Kerberos network authentication service as specified by [IETF RFC 4120] can be applied. In [IETF RFC 2712] additional TLS cipher suites are defined to support Kerberos based authentication.

How the TLS endpoints interface with the trusted third-party server and which information elements are exchanged between the TLS endpoint and the trusted third-party server is out of scope of this Recommendation.

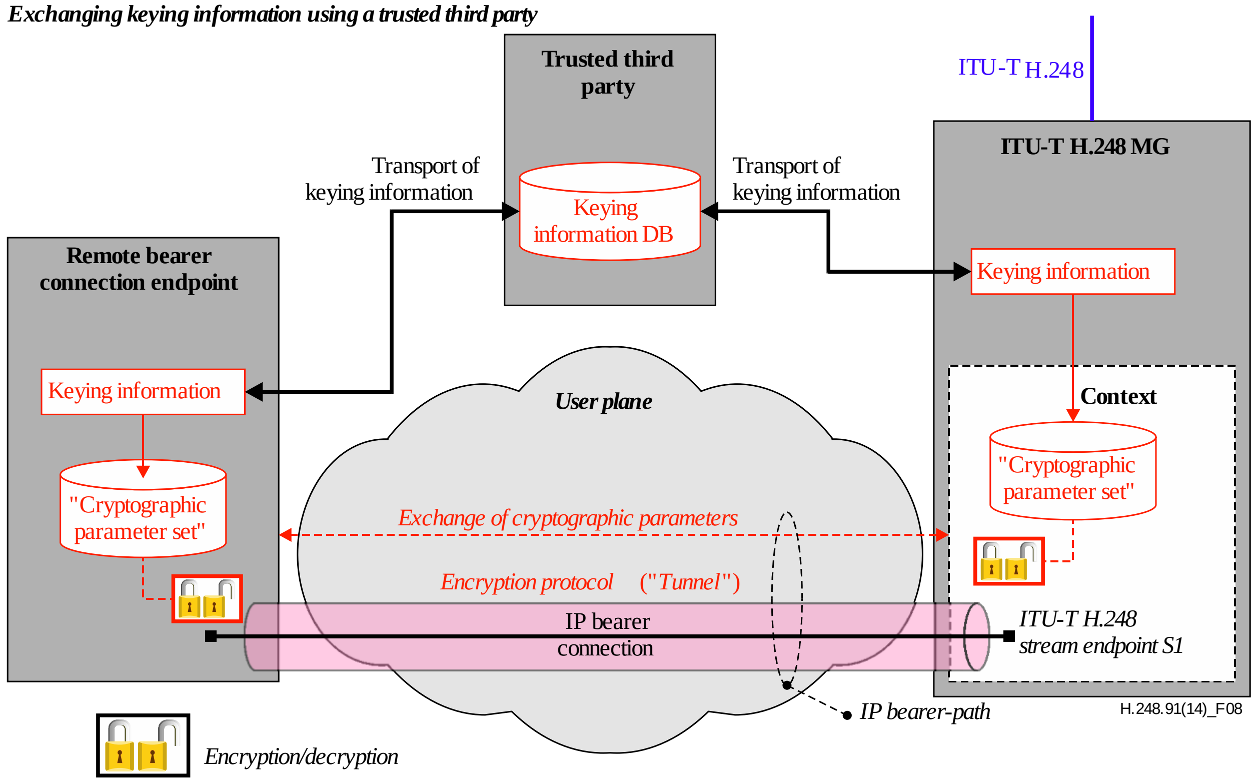


Figure 8 – Generic ITU-T H.248 model for bearer security – exchange of keying information using a third-party server

TLS profiles may define one or more cipher suites where involvement of such a trusted third party is required.

To support such cipher suites, the following requirements apply:

R-8.3.5/1: The MG is required to support related cipher suites.

R-8.3.5/2: The MG is required to support interfacing to a trusted third party server infrastructure.

NOTE – This requirement might depend on other conditions, e.g., for the Kerberos TLS-cipher suites only the TLS-client interacts with the Kerberos server.

R-8.3.5/3: The MG is required to select the trusted third party authentication service (either call-dependent or call-independent).

8.4 Renegotiation of security parameters

R-8.4/1: The MG is recommended to support the renegotiation procedures for the security parameters as specified in [IETF RFC 5246]. This requirement is applicable for the TLS-client as well as for the TLS-server implementation. The MGC is required to be able to audit the MG's capability for renegotiation.

R-8.4/2: The MGC is required to be able to instruct the MG whether and when a renegotiation is required to be initiated by the MG.

R-8.4/3: In case that during the renegotiation the authentication of the remote TLS endpoint fails, the MG is required to regard the remote endpoint as not authenticated and the related basic procedures shall apply.

R-8.4/4: In case the renegotiation fails, the MG is required to follow the basic error procedures.

8.5 Termination of the TLS/TCP session

8.5.1 Termination by remote TLS endpoint

The termination of a TLS/TCP-session may be initiated by both TLS/TCP-endpoints. When terminating a session the initiating endpoint sends a TLS *close_notify* alert to the remote side.

R-8.5.1/1: On reception of a TLS *close_notify* alert, the MG is required to close the TLS session according to the procedures defined in [IETF RFC 5246].

8.5.2 Abnormal termination by remote TLS endpoint

R-8.5.2/1: On reception of a TLS fatal alert message, the MG is required to close the TLS session according to the procedures defined in [IETF RFC 5246].

8.5.3 Abnormal termination by local TLS endpoint

R-8.5.3/1: In case the MG detects a condition which requires the TLS session to be terminated, the procedures defined in [IETF RFC 5246] are required to be followed to terminate the TLS session.

8.5.4 Notification of MGC about TLS session termination

R-8.5.4/1: The MGC may request to be explicitly notified about normally and abnormally released TLS sessions.

8.6 Reporting unsuccessful TLS connection set-up

R-8.6/1: In case the MG detects a non-recoverable error during the TLS-handshake, the same procedure of clause 8.5.3, R-8.5.3/1 is required to be followed.

8.7 TLS statistics

R-8.7/1: The MG is required to collect TLS-related statistics.

NOTE – Performance metrics related to the TLS record layer are typically of primary interest. Such as ITU-T H.248 statistics related to the sent and received volume of the TLS traffic at that protocol layer.

R-8.7/2: The MGC is required to be able to retrieve the statistics collected by the MG.

8.7.1 Note to MG transfer delay related metrics

The MG *packet transfer delay* τ_{TD} is the time difference between the entry and exit event of an individual packet in the user plane. Performance metric *L4/IP packet transfer delay* $\tau_{TD,L4}$ would be of primary interest in case of the considered TLS interworking models of ITU-T H.248 IP-IP gateways according clause 6.2.1 of [ITU-T H.248.90]. It is a basic performance metric because there might be significant differences behind the various TLS interworking use cases (e.g., an estimated qualitative relation of "$\tau_{TD,L4,withoutTLS} < \tau_{TD,L4,TLS\text{-}to\text{-}TLS} < \tau_{TD,L4,TLS\text{-}to\text{-}non\text{-}TLS} \ll \tau_{TD,L4,TLS\text{-}to\text{-}TLS*}$" due to expected MG processing involvement).

However, such a performance metric may not be observed by the ITU-T H.248 MG itself (due to the relation to the MG external interfaces). There are consequently not any correspondent ITU-T H.248 statistics supported. But, there are other mechanisms such as via network management capabilities which may be used to measure and report MG delay metrics.

8.8 Auditing of TLS related capabilities by the MGC

R-8.8/1: The MGC is required to be able to audit the TLS-related capabilities of the MG. This may comprise the following characteristics:

– entire TLS profiles:
  ○ supported TLS domain profile(s)
– and/or individual TLS profile elements:
  ○ supported TLS-versions
  ○ supported cipher suites
  ○ supported compression methods
  ○ support for resumption and renegotiation

9 Performance and resource aspects

R-9/1: When defining a TLS profile, attention should be paid to the performance and the resource aspects in the MG.

Asymmetric encryption methods as defined through the cipher suites, compression methods and the potential use of resumption significantly affect the processing resources required by the MG per TLS session. Attention should be paid for those performance aspects when defining the TLS profile.

NOTE – Clause 8.7.1 indicates possible impact on MG transfer delay of TLS traffic.

10 ITU-T H.248 profile specification guidelines

This clause provides guidelines for ITU-T H.248 profile specifications. The structure follows the profile template defined and described in Appendix III of [ITU-T H.248.1].

The template elements that are not applicable in this Recommendation are indicated by "*Subject to profile specification*".

Profile guidelines are primarily dependent on the concerned network configuration and use case. Therefore, the guidelines in this clause are in principle conditional. Two exemplary use cases are considered (as described in Appendix I), termed as capability set 'A' (CS_A) and capability set 'B' (CS_B).

10.1 Profile identification

Subject to profile specification.

10.2 Summary

Subject to profile specification.

10.3 Gateway control protocol version

Subject to profile specification.

10.4 Connection model

Maximum number of contexts:	*Subject to profile specification.*
Maximum number of terminations per context:	*Subject to profile specification.* Examples: IF CS_A THEN "2". IF CS_B THEN "2".
Allowed termination type combinations in a context:	*Subject to profile specification.*

10.5 Context attributes

Subject to profile specification.

10.6 Terminations

Subject to profile specification.

10.7 Descriptors

10.7.1 TerminationState Descriptor

Subject to profile specification.

10.7.2 Stream Descriptor

Subject to profile specification.

10.7.3 Events Descriptor

IF CS_A OR CS_B THEN following table:

Events settable on termination types and stream types:	Yes		
If yes	**Event ID**	**Termination type**	**Stream type**
	See clause 10.14.3.1 • tlsbsc/BNCChange	ALL except ROOT	TLS
	See clause 10.14.3.3 • tlsm/mgea	ALL except ROOT	TLS
	See clause 10.14.3.5 • tcpbcc/BNCChange	ALL except ROOT	ANY (if TCP)
	See clause 10.14.3.7 • tcphp/rnat	ALL except ROOT	ANY (if TCP)

All other aspects related to Events Descriptor (e.g., EventBuffer Control, KeepActive, Notification Behaviour) are "*Subject to profile specification*".

10.7.4 EventBuffer Descriptor

Subject to profile specification.

10.7.5 Signals Descriptor

IF CS_A OR CS_B THEN following table:

The setting of signals is dependent on termination or streams types:		Yes	
If yes	**Signal ID**	**Termination Type**	**Stream Type/ID**
	See clause 10.14.3.1 • tlsbsc/EstBNC • tlsbsc/RelBNC	ALL except ROOT	TLS
	See clause 10.14.3.3 • tlsm/mgcea	ALL except ROOT	TLS
	See clause 10.14.3.5 • tcpbcc/EstBNC • tcpbcc/RelBNC	ALL except ROOT	ANY (if TCP)

All other aspects related to Signals Descriptor (e.g., Signal Direction, Signal List) are "*Subject to profile specification*".

10.7.6 DigitMap Descriptor

Subject to profile specification.

10.7.7 Statistics Descriptor

IF CS_A THEN none.

IF CS_B THEN the following table entries:

Statistics supported on:	Both (i.e., stream and termination level)

Statistics reported on Subtract:	Yes	
If yes	**Statistic IDs reported**	tlstv/… (see clause 10.14.3.4) If TCP: tcphp/… (see clause 10.14.3.7) tcptv/… (see clause 10.14.3.8) tcpccm/… (see clause 10.14.3.9) tcpcqm/… (see clause 10.14.3.10) tcprm/… (see clause 10.14.3.11)

10.7.8 ObservedEvents Descriptor

Subject to profile specification.

10.7.9 Topology Descriptor

Subject to profile specification.

10.7.10 Error Descriptor

Subject to profile specification.

NOTE – The TLS session maintenance package [ITU-T H.248.90] may be used for enhanced abnormal TLS session handling (but this is beyond the example capability sets CS_A and CS_B).

10.8 Command API

NOTE – It is assumed that an Error Descriptor may be returned in any command reply.

10.8.1 Add

Subject to profile specification.

10.8.2 Modify

Subject to profile specification.

10.8.3 Subtract

Subject to profile specification.

10.8.4 Move

Subject to profile specification.

10.8.5 AuditValue

Subject to profile specification.

10.8.6 AuditCapabilities

Subject to profile specification.

10.8.7 Notify

Subject to profile specification.

10.8.8 ServiceChange

Subject to profile specification.

10.8.9 Manipulating and auditing context attributes

Subject to profile specification.

10.9 Generic command syntax and encoding

Subject to profile specification.

10.10 Transactions

Subject to profile specification.

NOTE – There is no impact on Transactions.

10.11 Messages

Subject to profile specification.

10.12 Transport

Subject to profile specification.

NOTE – Usage of bearer security may demand for a secured ITU-T H.248 transport mode, too.

10.13 Security

Subject to profile specification.

NOTE – In providing details in the security clause, one should consider whether the ITU-T H.248 MG might be a potential point of security attacks (due to possible security threats at IP, TCP and/or TLS layer).

10.14 Packages

10.14.1 Mandatory packages

Mandatory: specifies the packages that shall be supported in this profile.

Examples:

IF CS_A OR CS_B THEN "following table":

Mandatory packages:			
Package name	**Package ID**	**Version**	**Termination Types Supported**
"TLS basic session control package" [ITU-T H.248.90]	tlsbsc (0x0117)	v1	TLS
"TCP basic connection control package" [ITU-T H.248.89]	tcpbcc (0x0115)	v1	ANY (if TCP)

10.14.2 Optional packages

Examples:

IF CS_A OR CS_B THEN "following table":

Optional packages:			
Package name	**Package ID**	**Version**	**Termination Types Supported**
"Stream endpoint interlinkage package" [ITU-T H.248.92]	seplink (0x011b)	v1	TLS, TCP

Examples:

IF CS_B THEN "following table":

Optional packages:			
Package name	**Package ID**	**Version**	**Termination Types Supported**
"TLS capability negotiation package" [ITU-T H.248.90]	tlscn (0x0118)	v1	TLS
"TLS session maintenance package" [ITU-T H.248.90]	tlsm (0x0119)	v1	TLS
"TLS traffic volume metrics package" [ITU-T H.248.90]	tlstv (0x011a)	v1	TLS
"NAT-traversal peer-to-peer package" [ITU-T H.248.84]	nattp2p (0x010d)	v1	ANY (if TCP)
"TCP hole punching package" [ITU-T H.248.84]	tcphp (0x010e)	v1	ANY (if TCP)
"TCP traffic volume metrics package" [ITU-T H.248.84]	tcptv (0x010f)	v1	ANY (if TCP)
"TCP connection control metrics package" [ITU-T H.248.84]	tcpccm (0x0110)	v1	ANY (if TCP)
"TCP connection quality metrics package" [ITU-T H.248.84]	tcpcqm (0x0111)	v1	ANY (if TCP)
"TCP retransmission metrics package" [ITU-T H.248.89]	tcprm (0x0116)	v1	ANY (if TCP)

10.14.3 Package usage information

The following clauses contain a non-exhaustive list of package usage indications.

10.14.3.1 TLS basic session control package

Example:

IF CS_A OR CS_B THEN "usage detail see table …":

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**	**Termination/Stream Types Supported**
bceb (0x0001)	O (Note)	ADD, MOD	ALL	"Un-blocked "	TLS
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
EstBNC (0x0001)	M	ADD, MOD		–	
RelBNC (0x0002)	M	ADD, MOD		–	
Events	**Mandatory/ Optional**	**Used in command**			
BNCChange (0x0001)	M	ADD, MOD			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				
NOTE – Required for e.g., too early incoming TLS messages (due to security threat), or delayed TLS session establishment (due to multiple SDP offer/answer cycles, ITU-T H.248 two-stage resource reservation, to await firstly successful L4 connectivity, etc.).					

10.14.3.2 TLS capability negotiation package

Example:

IF CS_B THEN "usage detail see table …":

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**	**Termination/Stream Types Supported**
dpid (0x0001)	O	ADD, MOD, MOV	ALL	–	TLS
tlsv (0x0002)	O	ADD, MOD, MOV	ALL	"0303" (Note)	TLS
cs (0x0003)	O	ADD, MOD, MOV	ALL	–	TLS
cm (0x0004)	O	ADD, MOD, MOV	ALL	–	TLS

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
srsc (0x0005)	O	ADD, MOD, MOV	ALL	FALSE	TLS
rp (0x0006)	O	ADD, MOD, MOV	ALL	0	TLS
car (0x0007)	O	ADD, MOD, MOV	ALL	–	TLS
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				
NOTE – This codepoint relates to "TLS v1.2".					

10.14.3.3 TLS session maintenance package

Example:

IF CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
mgcea (0x0001)	O	ADD, MOD		–	
Events	**Mandatory/ Optional**	**Used in command**			
mgea (0x0001)	O	ADD, MOD			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

10.14.3.4 TLS traffic volume metrics package

Example:

IF CS_B THEN "usage detail see table …":

Properties	**Mandatory/ Optional**	**Used in command**	**Supported values**	**Provisioned value**	**Termination/Stream Types Supported**
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None.	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
recadfrag (0x0001)	Not supported.	–	–		–
sentadfrag (0x0002)	Not supported.	–	–		–
rectmfrag (0x0003)	Not supported.	–	–		–
senttmfrag (0x0004)	Not supported.	–	–		–
recado (0x0005)	M	AUDITVALUE, SUB	ALL		TLS
sentado (0x0006)	M	AUDITVALUE, SUB	ALL		TLS
rectmo (0x0007)	Not supported.	–	–		–
senttmo (0x0008)	Not supported.	–	–		–
recadpduo (0x0009)	M	AUDITVALUE, SUB	ALL		TLS
sentadpduo (0x000a)	M	AUDITVALUE, SUB	ALL		TLS
rectmpduo (0x000b)	Not supported.	–	–		–
senttmpduo (0x000c)	Not supported.	–	–		–
recadpco (0x000d)	Not supported.	–	–		–
sentadpco (0x000e)	Not supported.	–	–		–
rectmpco (0x000f)	Not supported.	–	–		–

Statistics	Mandatory/ Optional	Used in command	Supported values	Termination/Stream Types Supported
senttmpco (0x0010)	Not supported.	–	–	–
recadcfo (0x0011)	Not supported.	–	–	–
sentadcfo (0x0012)	Not supported.	–	–	–
rectmcfo (0x0013)	Not supported.	–	–	–
senttmcfo (0x0014)	Not supported.	–	–	–
Error codes	**Mandatory/Optional**			
None.	–			

10.14.3.5 TCP basic connection control package

Example:

IF CS_A OR CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
bceb (0x0001)	O (Note 1)	ADD, MOD	ALL	"Unblocked"	ANY (if TCP)
ori (0x0002)	O (Note 2)	ADD, MOD	ALL	"False"	ANY (if TCP)
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
EstBNC (0x0001)	M	ADD, MOD		–	
RelBNC (0x0002)	M	ADD, MOD		–	
Events	**Mandatory/ Optional**	**Used in command**			
BNCChange (0x0001)	M	ADD, MOD			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				
NOTE 1 – Required for e.g., too early incoming TCP packets (due to security threats), or delayed TLS session establishment (due to multiple SDP offer/answer cycles, ITU-T H.248 two-stage resource reservation, to decouple the establishment of the two TCP connection segments (in case of TCP proxy), etc.). NOTE 2 – Only required for services with one-way TCP connection release support.					

10.14.3.6 NAT-traversal peer-to-peer package

Example:

IF CS_B THEN "usage detail see table …":

<table>
<tr><th>Properties</th><th>Mandatory/ Optional</th><th>Used in command</th><th>Supported values</th><th>Provisioned value</th><th>Termination/Stream Types Supported</th></tr>
<tr><td>None.</td><td>–</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
<tr><th>Signals</th><th>Mandatory/ Optional</th><th colspan="2">Used in command</th><th colspan="2">Duration provisioned value</th></tr>
<tr><td>None.</td><td>–</td><td colspan="2">–</td><td colspan="2">–</td></tr>
<tr><th>Events</th><th>Mandatory/ Optional</th><th colspan="4">Used in command</th></tr>
<tr><td>rnatip (0x0001)</td><td>O</td><td colspan="4">ADD,
MOD</td></tr>
<tr><th>Statistics</th><th>Mandatory/ Optional</th><th>Used in command</th><th colspan="2">Supported values</th><th>Termination/Stream Types Supported</th></tr>
<tr><td>None.</td><td>–</td><td>–</td><td colspan="2">–</td><td>–</td></tr>
<tr><th>Error codes</th><th colspan="5">Mandatory/Optional</th></tr>
<tr><td>None.</td><td colspan="5">–</td></tr>
</table>

10.14.3.7 TCP hole punching package

Example:

IF CS_B THEN "usage detail see table …":

<table>
<tr><th>Properties</th><th>Mandatory/ Optional</th><th>Used in command</th><th>Supported values</th><th>Provisioned value</th><th>Termination/Stream Types Supported</th></tr>
<tr><td>None.</td><td>–</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
<tr><th>Signals</th><th>Mandatory/ Optional</th><th colspan="2">Used in command</th><th colspan="2">Duration provisioned value</th></tr>
<tr><td>None.</td><td>–</td><td colspan="2">–</td><td colspan="2">–</td></tr>
<tr><th>Events</th><th>Mandatory/ Optional</th><th colspan="4">Used in command</th></tr>
<tr><td>rnat (0x0001)</td><td>O</td><td colspan="4">ADD,
MOD</td></tr>
<tr><th>Statistics</th><th>Mandatory/ Optional</th><th>Used in command</th><th colspan="2">Supported values</th><th>Termination/Stream Types Supported</th></tr>
<tr><td>rstrx (0x0001)</td><td>O</td><td>AUDITVALUE,
SUB</td><td colspan="2">ALL</td><td>TCP</td></tr>
<tr><td>synrx (0x0002)</td><td>O</td><td>AUDITVALUE,
SUB</td><td colspan="2">ALL</td><td>TCP</td></tr>
<tr><th>Error codes</th><th colspan="5">Mandatory/Optional</th></tr>
<tr><td>None.</td><td colspan="5">–</td></tr>
</table>

10.14.3.8 TCP traffic volume metrics package

Example:

IF CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None.	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
tcpos (0x0001)	O	SUB	ALL		TCP
tcpor (0x0002)	O	SUB	ALL		TCP
tcpps (0x0003)	Not supported.	–	–		–
tcppr (0x0004)	Not supported.	–	–		–
Error codes	**Mandatory/Optional**				
None.	–				

10.14.3.9 TCP connection control metrics package

Example:

IF CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None.	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
tcpest (0x0001)	M	SUB	ALL		TCP

Statistics	Mandatory/ Optional	Used in command	Supported values	Termination/Stream Types Supported
tcpsyntx (0x0002)	O	SUB	ALL	TCP
tcpsynrx (0x0003)	O	SUB	ALL	TCP
Error codes	**Mandatory/Optional**			
None.	–			

10.14.3.10 TCP connection quality metrics package

Example:

IF CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None.	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
tcprttest (0x0001)	O	SUB	ALL		TCP
Error codes	**Mandatory/Optional**				
None.	–				

10.14.3.11 TCP retransmission metrics package

Example:

IF CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
None.	–	–	–	–	–
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None.	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			

Statistics	Mandatory/ Optional	Used in command	Supported values	Termination/Stream Types Supported
tcpros (0x0001)	Not supported.	–	–	–
tcprps (0x0002)	O	SUB	ALL	TCP
Error codes	**Mandatory/Optional**			
None.	–			

10.14.3.12 Stream endpoint interlinkage package

Example:

IF CS_A OR CS_B THEN "usage detail see table …":

Properties	Mandatory/ Optional	Used in command	Supported values	Provisioned value	Termination/Stream Types Supported
linktopo (0x0001)	O	ADD, MOD	only TLS and TCP endpoints	empty list	TLS, TCP
Signals	**Mandatory/ Optional**	**Used in command**		**Duration provisioned value**	
None.	–	–		–	
Events	**Mandatory/ Optional**	**Used in command**			
None.	–	–			
Statistics	**Mandatory/ Optional**	**Used in command**	**Supported values**		**Termination/Stream Types Supported**
None.	–	–	–		–
Error codes	**Mandatory/Optional**				
488	–				

10.15 Mandatory support of SDP and ITU-T H.248.1 Annex C information elements

At least the following:

Supported Annex C and SDP information elements		
Information element	**Annex C support**	**SDP support**
"m="-line <proto>	not supported (in this example)	Value(s): ALL IANA registered codepoints with "TLS" protocol Purpose: bearer type indication ("TLS security session" Dependent on required MG behaviour for "TLS/L4 enabled terminations" (here: L4 = 'TCP'): – application-aware: "<*L4*>/TLS/<*application*>" – application-agnostic: "<*L4*>/TLS/–"
		Value(s): ALL IANA registered codepoints with "TCP" protocol Purpose: bearer type indication ("TCP bearer connection" Dependent on required MG behaviour for "TCP enabled terminations": – application-aware: "TCP/<*application*>" – application-agnostic: "TCP/–"
"a=fingerprint:"	not supported (in this example)	Value(s): all Purpose: TLS authentication procedures

Rest: subject to profile specification.

10.16 Optional support of SDP and ITU-T H.248.1 Annex C information elements

At least the following:

Supported Annex C and SDP information elements		
Information element	**Annex C support**	**SDP support**
"a=setup:"	not supported (in this example)	IF CS_B THEN "TCP merge/relay mode" indication (for L3/L4 NAT-T) (Note)
NOTE – Usage of this SDP attribute is defined in clause 13 of [ITU-T H.248.84].		

Rest: subject to profile specification.

10.17 Procedures

The initial release of this Recommendation focuses on the previous profile elements. Specific guidelines for this clause are for further studies.

Appendix I

Use case specific capability sets – Two examples

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

I.1 Overview

Profile content is mainly use case dependent as outlined in clause 1. In order to demonstrate profile specification guidelines in clause 10, this Recommendation considers two exemplary use cases:

– Capability set 'A' (CS_A):
  1. a *TCP-to-TCP media gateway*,
  2. connected to a single TLS domain,
  3. supporting TLS-to-non-TLS interworking and TLS-to-TLS transparent forwarding,
  4. optional support of stream endpoint interlinkage capability with regards to the establishment and release of bearer entities TCP, TLS and combined TLS/TCP (in addition to MGC strict control of individual stream endpoints);
  5. only support of a single TLS authentication principle,
  6. only support of certificates issued by a certification authority;
  7. only support of a minimum, fixed TLS profile (without any options),
  8. any orthogonal L3/L4 NAT traversal support is disregarded, and
  9. the MGC should be offloaded as best as possible from TLS security session and TCP bearer connection control.

– Capability set 'B' (CS_B):
  1. a *TCP-to-TCP media gateway*,
  2. support of multiple TLS domains,
  3. supporting TLS-to-non-TLS interworking, TLS-to-TLS transparent forwarding and additional TLS-to-TLS* interworking,
  4. optional support of stream endpoint interlinkage capability with regards to the establishment and release of bearer entities TCP, TLS and combined TLS/TCP (in addition to MGC strict control of individual stream endpoints)
  5. only support of a single TLS authentication principle,
  6. support of self-signed certificates besides certificates issued by a certification authority;
  7. support of L3/L4 NAT traversal,
  8. optional MGC-influenced TLS session negotiations, and
  9. optional support of the basic TLS performance monitoring (limited on bit-rate related traffic volume measurements at the two measurement points "L4 – TLS record layer" and "TLS – application layer") and TCP layer performance monitoring.

Capability set 'B' (CS_B) is therefore a superset of capability set 'A' (CS_A).

Tables I.I and I.2 illustrate sets of requirements (based on clauses 6 to 9) for profiling the two gateway types.

Table I.1 – MG example for capability set 'A' (CS_A)

Functional area	Capabilities
Requirements for control of the MG mode of operation: – TLS transport mode – MG mode of operation for case of TLS-over-TCP transport	 – R-6.1/1, – R-6.2/1, R-6.2/2, R-6.2/3, R-6.2/4, R-6.2/5
Requirements given by a TLS Profile concept: – Requirements to a TLS profile as such – Requirements to elements of TLS profiles	 – R-7.1/1, – R-7.2/1, R-7.2/2, R-7.2/3, R-7.2/4, R-7.2/6, R-7.2/7 (Note)
Requirements on TLS procedures: – Selection of the TLS domain – Client/Server Mode – Behavioural Requirements for Authentication – Renegotiation of security parameters – Termination of the TLS/TCP session – Reporting unsuccessful TLS connection setup – TLS Statistics – Auditing of TLS related capabilities by the MGC	 – R-8.1/2 (single TLS domain case), – R-8.2.1/all, R-8.2.2/1, – R-8.3.1/all, R-8.3.2/1, R-8.3.3/all, R-8.3.3.1/all – R-8.4/1, R-8.4/3, R-8.4/4, – R-8.5.all/all, – R-8.6/1, – – – –
Performance and resource aspects	–
NOTE – No support of TLS session resumption.	

Table I.2 – MG example for capability set 'B' (CS_B)

Functional area	Capabilities
Requirements for control of the MG mode of operation: – TLS transport mode – MG mode of operation for case of TLS-over-TCP transport	 – R-6.1/1, – R-6.2/1, R-6.2/2, R-6.2/3, R-6.2/4, R-6.2/5
Requirements given by a TLS Profile concept: – Requirements to a TLS profile as such – Requirements to elements of TLS profiles	 – R-7.1/1, – R-7.2/1, R-7.2/2, R-7.2/3, R-7.2/4, R-7.2/6, R-7.2/7 (Note)
Requirements on TLS procedures: – Selection of the TLS domain – Client/Server Mode – Behavioural Requirements for Authentication – Renegotiation of security parameters – Termination of the TLS/TCP session – Reporting unsuccessful TLS connection setup – TLS Statistics – Auditing of TLS related capabilities by the MGC	 – R-8.1/1, R-8.1/3, R-8.1/4, – R-8.2.1/all, R-8.2.2/1, – R-8.3.1/all, R-8.3.2/1, R-8.3.3/all, R-8.3.3.1/all, R-8.3.3.2/all, – R-8.4/1, R-8.4/2, R-8.4/3, R-8.4/4, – R-8.5.all/all, – R-8.6/1, – R-8.7/1, R-8.7/2, – R-8.8/1,
Performance and resource aspects	– R-9/1
NOTE – No support of TLS session resumption.	

Bibliography

[b-ITU-T H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package.*

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*.

[b-IETF RFC 5914] IETF RFC 5914 (2010), *Trust Anchor Format.*

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