

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

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/>.

© ITU 2015

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope.....	1
2 References.....	2
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	3
4 Abbreviations and acronyms	3
5 Conventions	3
6 Requirements for control the MG mode of operation	4
6.1 TLS transport mode	4
6.2 MG mode of operation for case of TLS-over-TCP transport	4
7 Requirements given by a TLS Profile concept	6
7.1 Requirements to such a TLS profile	6
7.2 Requirements to elements of TLS profiles	6
8 Requirements on TLS procedures	7
8.1 Selection of the TLS domain	7
8.2 Client/Server Mode	8
8.3 Behavioural requirements for authentication	9
8.4 Renegotiation of security parameters	13
8.5 Termination of the TLS/TCP session	14
8.6 Reporting unsuccessful TLS connection set-up	14
8.7 TLS statistics	14
8.8 Auditing of TLS related capabilities by the MGC	15
9 Performance and resource aspects	15
10 ITU-T H.248 profile specification guidelines	15
10.1 Profile identification	15
10.2 Summary.....	15
10.3 Gateway control protocol version	15
10.4 Connection model.....	16
10.5 Context attributes.....	16
10.6 Terminations.....	16
10.7 Descriptors.....	16
10.8 Command API.....	17
10.9 Generic command syntax and encoding.....	18
10.10 Transactions.....	18
10.11 Messages.....	18
10.12 Transport.....	18
10.13 Security.....	18



	Page
10.14 Packages	18
10.15 Mandatory support of SDP and ITU-T H.248.1 Annex C information elements	28
10.16 Optional support of SDP and ITU-T H.248.1 Annex C information elements	28
10.17 Procedures	28
Appendix I – Use case specific capability sets – Two examples	29
I.1 Overview	29
Bibliography	31

Copyright © 2014 ITU-T. All rights reserved.

Recommendation ITU-T H.248.91

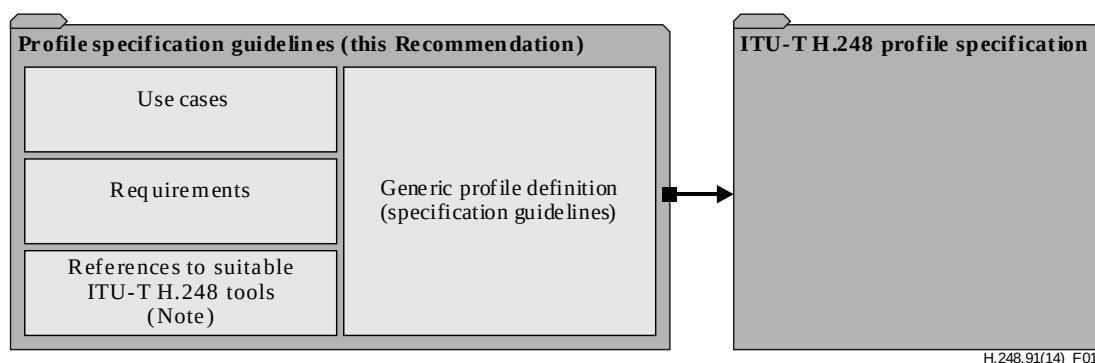
Gateway control protocol: Guidelines on the use of ITU-T H.248 capabilities for transport security in TLS networks in ITU-T H.248 profiles

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".

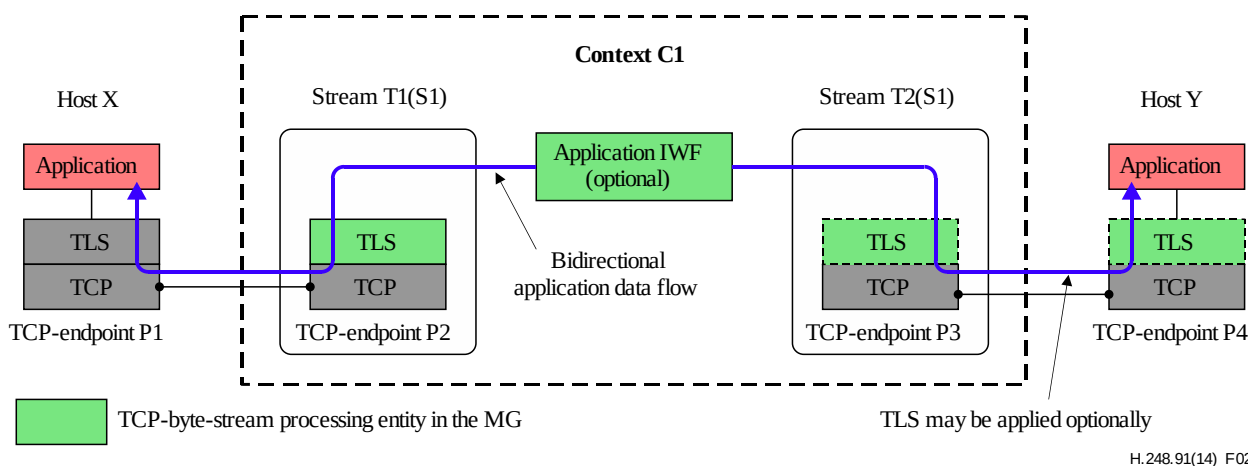


Figure 2 – TCP-byte stream processing entities located in the MG

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.

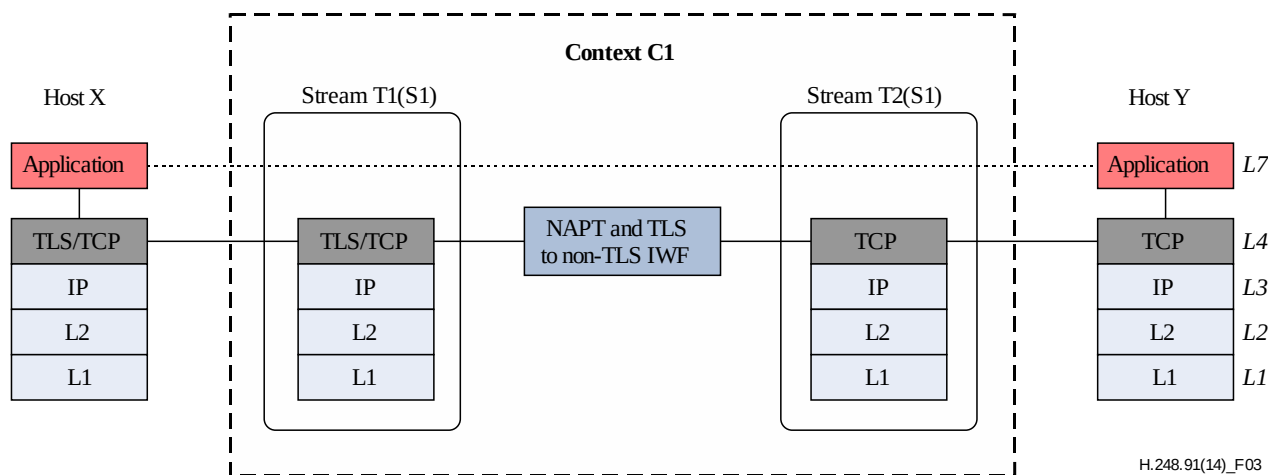


Figure 3 – "Application agnostic" TCP-proxy with TLS to non-TLS interworking

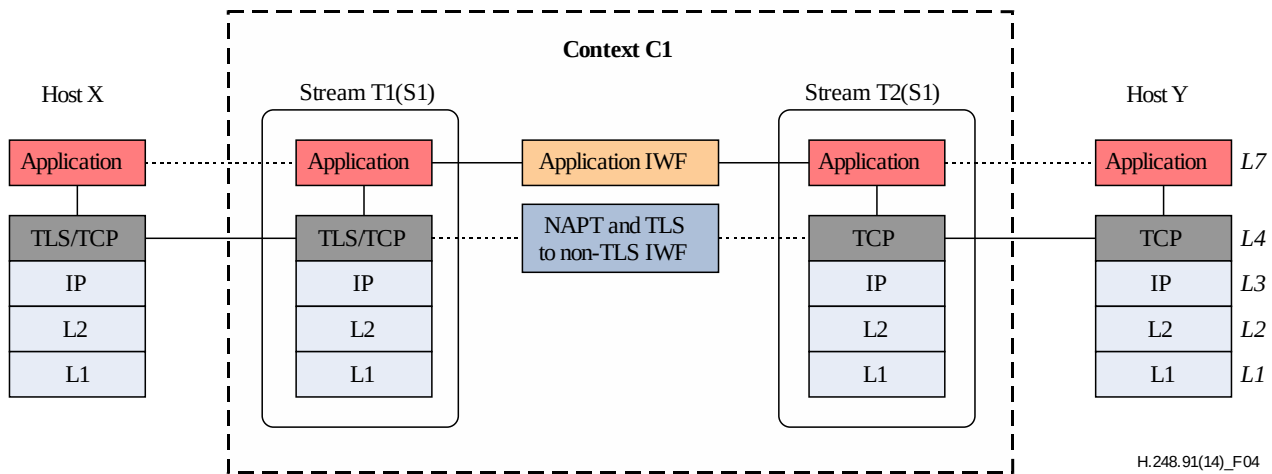


Figure 4 – "Application aware" TCP-proxy with TLS to non-TLS interworking

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.