# ETSI TS 124 322 V15.0.0 (2018-06)


**Universal Mobile Telecommunications System (UMTS);**
**LTE;**
**Tunnelling of IP Multimedia Subsystem (IMS) services over restrictive access networks;**
**Stage 3**
**(3GPP TS 24.322 version 15.0.0 Release 15)**

Reference
RTS/TSGC-0124322vf00

Keywords
LTE,UMTS

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

# Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document specifies procedures and protocol elements for tunnelling of IMS traffic over restrictive access networks, specifically procedures and protocol elements for establishing, maintaining, and sending traffic via a firewall traversal tunnel between the UE and an enhanced firewall traversal function (EFTF) in the network. The present document is applicable to UE and EFTF.

The present document applies only to the case when the IMS traffic is not routed via EPC of a PLMN. Procedures for tunnelling of IMS traffic that is routed via EPC are specified in 3GPP TS 24.302 [3] annex F.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[3] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[4] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[5] IETF RFC 791 (September 1981): "Internet Protocol".

[6] IETF RFC 2131 (March 1997): "Dynamic Host Configuration Protocol".

[7] IETF RFC 2460 (December 1998): "Internet Protocol, Version 6 (IPv6) Specification".

[8] IETF RFC 2817 (May 2000): "Upgrading to TLS Within HTTP/1.1".

[9] IETF RFC 3736 (April 2004): "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[10] IETF RFC 4291 (February 2006): "IP Version 6 Addressing Architecture".

[11] IETF RFC 4862 (September 2007): "IPv6 Stateless Address Autoconfiguration".

[12] Void.

[13] Void.

[14] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Firewall traversal tunnel to IP network of IMS:** a TCP connection with TLS connection enabling passing of envelopes between UE in restrictive non-3GPP access network and EFTF, established in order to reach IP network of IP multimedia core network subsystem.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.229 [2] apply:

**IP multimedia core network subsystem**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.302 [3] apply:

**Restrictive non-3GPP access network type I**
**Restrictive non-3GPP access network type II**
**Restrictive non-3GPP access network**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.203 [4] apply:

**Enhanced firewall traversal function**

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

| | |
|---|---|
| EFTF | Enhanced firewall traversal function |
| FTT-IMS | Firewall traversal tunnel to IP network of IMS |
| HTTP | Hypertext transfer protocol |
| IMS | IP multimedia core network subsystem |
| TCP | Transmission control protocol |
| TLS | Transport layer security |
| URI | Uniform resource identifier |

# 4 UE – network protocols

## 4.1 General

In order to access to IMS via restrictive non-3GPP access network, the UE and the EFTF shall establish a firewall traversal tunnel to IP network of IMS (FTT-IMS) using the UE requested FTT-IMS establishment procedure according to subclause 5.2.

The UE and the EFTF shall send the IP packets using the IP packet transport FTT-IMS procedure according to subclause 5.3.

The UE and the EFTF shall use the IP protocol according to clause 6.

When FTT-IMS is no longer needed (e.g. if the UE deregistered from IMS), the UE shall perform the UE requested FTT-IMS release procedure according to subclause 5.4.

When FTT-IMS is no longer needed, the EFTF can perform the EFTF requested FTT-IMS release procedure according to subclause 5.5.

NOTE: Keep-alive functionality is not defined in this document. Keep-alive functionality defined in 3GPP TS 24.229 [2] can be used to maintain the FTT-IMS between the UE and the EFTF.

# 5 FTT-IMS protocol

## 5.1 General

The FTT-IMS protocol consists of the UE requested FTT-IMS establishment procedure, the IP packet transport FTT-IMS procedure, the UE requested FTT-IMS release procedure and the EFTF requested FTT-IMS release procedure.

## 5.2 UE requested FTT-IMS establishment procedure

### 5.2.1 General

The purpose of the UE requested FTT-IMS establishment procedure is to establish an FTT-IMS between the UE and the EFTF.

### 5.2.2 UE procedures

#### 5.2.2.1 UE requested FTT-IMS establishment procedure initiation

If the UE is not configured with an HTTP proxy address, the UE shall follow the procedures in subclause 5.2.2.2.

If the UE is configured with an HTTP proxy address, the UE shall follow the procedures in subclause 5.2.2.3.

NOTE: UE configuration of an HTTP proxy address is out of scope of 3GPP.

#### 5.2.2.2 UE requested FTT-IMS establishment procedure initiation via restrictive non-3GPP access network type I

In order to establish an FTT-IMS, the UE shall establish a TCP connection to the EFTF address and destination port 443.

If the TCP connection establishment is successful, the UE shall establish a TLS connection over the TCP connection according to the TLS profile specified in 3GPP TS 33.310 [14] annex E. If the EFTF address is a FQDN, the UE shall include a TLS extension of type "server_name" in the TLS client hello message according to the TLS profile specified in 3GPP TS 33.310 [14] annex E.

#### 5.2.2.3 UE requested FTT-IMS establishment procedure initiation via restrictive non-3GPP access network type II

If the UE is configured with HTTP proxy address, in order to establish an FTT-IMS, the UE shall send HTTP CONNECT request to the HTTP proxy address according to IETF RFC 2817 [8]. The UE shall populate Request-URI of the HTTP CONNECT request with the EFTF address and port 443.

Upon receiving HTTP 2xx response to HTTP CONNECT request, the UE shall establish TLS connection according to the TLS profile specified in 3GPP TS 33.310 [14] annex E over the TCP connection used for the HTTP CONNECT request transport. If the EFTF address is a FQDN, the UE shall include a TLS extension of type "server_name" in the TLS client hello message according to the TLS profile specified in 3GPP TS 33.310 [14] annex E.

#### 5.2.2.4 UE requested FTT-IMS establishment procedure accepted

When valid TLS Finished message is received over the TCP connection, the UE shall use the connection as the FTT-IMS.

### 5.2.3 EFTF procedures

The EFTF shall handle the TCP connection setup and the TLS connection establishment according to the TLS profile specified in 3GPP TS 33.310 [14] annex E.

When TLS Finished message is sent over the TCP connection according to the TLS profile specified in 3GPP TS 33.310 [14] annex E, the EFTF shall use the connection as the FTT-IMS.

# 5.3 IP packet transport FTT-IMS procedure

## 5.3.1 General

The purpose of the IP packet transport FTT-IMS procedure is to transport an IPv4 packet or IPv6 packet over an FTT-IMS.

## 5.3.2 UE procedures

### 5.3.2.1 IP packet sending

In order to send an IPv4 packet or IPv6 packet, the UE shall create an IP packet envelope according to subclause 7.1.2.2, and shall populate the IP packet field of the IP packet envelope with the IPv4 packet or the IPv6 packet and shall send the IP packet envelope as TLS application data over the FTT-IMS.

### 5.3.2.2 IP packet receiving

Upon receiving the IP packet envelope as TLS application data over the FTT-IMS, the UE shall:

- if the UE supports IPv4 and the field in the four most significant bits of the first octet of the IP packet field of the IP packet envelope according to subclause 7.1.2.2 contains 4, handle the IP packet as an IPv4 packet according to IETF RFC 791 [5];

- if the UE supports IPv6 and the field in the four most significant bits of the first octet of the IP packet field of the IP packet envelope according to subclause 7.1.2.2 contains 6, handle the IP packet as an IPv6 packet according to IETF RFC 2460 [7]; and

- if the field in the four most significant bits of the first octet of the IP packet field of the IP packet envelope according to subclause 7.1.2.2 indicates not supported IP version, discard the IP packet envelope.

NOTE: The field in the four most significant bits of the first octet of both the IPv4 packet and the IPv6 packet indicates the IP version.

## 5.3.3 EFTF procedures

### 5.3.3.1 IP packet sending

In order to send an IPv4 packet or IPv6 packet, the EFTF shall create an IP packet envelope according to subclause 7.1.2.2, and shall populate the IP packet field of the IP packet envelope with the IPv4 packet or the IPv6 packet and shall send the IP packet envelope as TLS application data over the FTT-IMS.

### 5.3.3.2 IP packet receiving

Upon receiving the IP packet envelope as TLS application data over the FTT-IMS, the EFTF shall:

- if the EFTF supports IPv4 and the field in the four most significant bits of the first octet of the IP packet field of the IP packet envelope according to subclause 7.1.2.2 contains 4, handle the IP packet as an IPv4 packet according to IETF RFC 791 [5];

- if the EFTF supports IPv6 and the field in the four most significant bits of the first octet of the IP packet field of the IP packet envelope according to subclause 7.1.2.2 contains 6, handle the IP packet as an IPv6 packet according to IETF RFC 2460 [7]; and

- if the field in the four most significant bits of the first octet of the IP packet field of the IP packet envelope according to subclause 7.1.2.2 indicates not supported IP version, discard the IP packet envelope.

NOTE: The field in the four most significant bits of the first octet of both the IPv4 packet and the IPv6 packet indicates the IP version.

## 5.4 UE requested FTT-IMS release procedure

### 5.4.1 General

The purpose of the UE requested FTT-IMS release procedure is to release an FTT-IMS when FTT-IMS is no longer needed.

### 5.4.2 UE procedures

In order to release the FTT-IMS, the UE shall send TLS close_notify alert according to the TLS profile specified in 3GPP TS 33.310 [14] annex E

### 5.4.3 EFTF procedures

The EFTF shall handle the TLS close_notify alert according to the TLS profile specified in 3GPP TS 33.310 [14] annex E.

## 5.5 EFTF requested FTT-IMS release procedure

### 5.5.1 General

The purpose of the EFTF requested FTT-IMS release procedure is to release an FTT-IMS when FTT-IMS is no longer needed.

### 5.5.2 EFTF procedures

In order to release the FTT-IMS, the EFTF shall send TLS close_notify alert according to the TLS profile specified in 3GPP TS 33.310 [14] annex E.

### 5.5.3 UE procedures

The UE shall handle the TLS close_notify alert according to the TLS profile specified in 3GPP TS 33.310 [14] annex E.

## 5.6 Procedure for unknown FTT-IMS envelope types

### 5.6.1 General

The purpose of this procedure is forward compatibility.

### 5.6.2 UE procedures

Upon receiving a generic FTT-IMS envelope with the type field indicating an envelope type other than the envelope types defined by this version of specification in subclause 7.1.2, the UE shall discard the generic FTT-IMS envelope.

### 5.6.3 EFTF procedures

Upon receiving a generic FTT-IMS envelope with the type field indicating an envelope type other than the envelope types defined by this version of specification in subclause 7.1.2, the EFTF shall discard the generic FTT-IMS envelope.

# 6 IP roles and IP based procedures

## 6.1 General

This subclause describes IP roles and IP based procedures.

## 6.2 IP roles

### 6.2.1 UE procedures

If IPv4 is supported, the UE shall support acting as host according to IETF RFC 791 [5].

If IPv6 is supported, the UE shall support acting as host according to IETF RFC 2460 [7].

### 6.2.2 EFTF procedures

If IPv4 is supported, the EFTF shall support acting as gateway according to IETF RFC 791 [5].

If IPv6 is supported, the EFTF shall support acting as router according to IETF RFC 2460 [7].

## 6.3 Inner IP address assignment procedure

### 6.3.1 UE procedures

If the UE has a network interface with a universally administered MAC address, the UE shall use a universally administered MAC address of a network interface of the UE as the UE FTT-IMS MAC address. If the UE does not have a network interface with a universally administered MAC address, the UE shall use a locally administered MAC address where the least significant bit of the last octet is set to zero as the UE FTT-IMS MAC address.

If IPv4 is supported, the UE shall support acting as DHCPv4 client according to IETF RFC 2131 [6].

If IPv6 is supported, the UE shall support acting as host supporting the IPv6 stateless address autoconfiguration according to IETF RFC 4862 [11].

Once the FTT-IMS is established, the UE shall:

1) if the UE needs IPv4 connectivity, request IPv4 address using DHCPv4 according to IETF RFC 2131 [6]. The UE shall use the htype, hlen, chaddr according to the UE FTT-IMS MAC address; and

2) if the UE needs IPv6 connectivity, generate IPv6 address using IPv6 stateless address autoconfiguration according to IETF RFC 4862 [11]. The UE shall create a link-local address according to IETF RFC 4291 [10] using the UE FTT-IMS MAC address.

NOTE 1: Further IPv6 configuration can be done using stateless DHCPv6 according to IETF RFC 3736 [9].

NOTE 2: DHCPv4 uses IPv4 as transport; IPv6 stateless address autoconfiguration uses IPv6 as transport and DHCPv6 uses IPv6 as transport. Thus, the DHCPv4 messages, IPv6 stateless address autoconfiguration messages and DHCPv6 messages are transported via the FTT-IMS using the IP packet transport FTT-IMS procedure according to subclause 5.3.

### 6.3.2 EFTF procedures

If IPv4 is supported, the EFTF shall support acting as DHCPv4 server according to IETF RFC 2131 [6]. When acting as DHCPv4 server, the EFTF shall handle each existing FTT-IMS as a different subnet.

If the EFTF has a network interface with a universally administered MAC address, the EFTF shall use a universally administered MAC address of a network interface of the EFTF as the EFTF FTT-IMS MAC address. If the EFTF does not have a network interface with a universally administered MAC address, the EFTF shall use a locally administered MAC address where the least significant bit of the last octet is set to one as the EFTF FTT-IMS MAC address.

If IPv6 is supported, the EFTF shall support acting as router supporting the IPv6 stateless address autoconfiguration according to IETF RFC 4862 [11]. The EFTF shall create a link-local address according to IETF RFC 4291 [10] using the EFTF FTT-IMS MAC address.

# 7 PDUs and parameters

## 7.1 PDUs and parameters specific to FTT-IMS protocol

### 7.1.1 General

The least significant bit of a field is represented by the lowest numbered bit of the highest numbered octet of the field. When the field extends over more than one octet, the order of bit values progressively decreases as the octet number increases.

Figure 7.1.1-1 shows an example of a field where the most significant bit of the field is marked MSB and the least significant bit of the field is marked LSB.

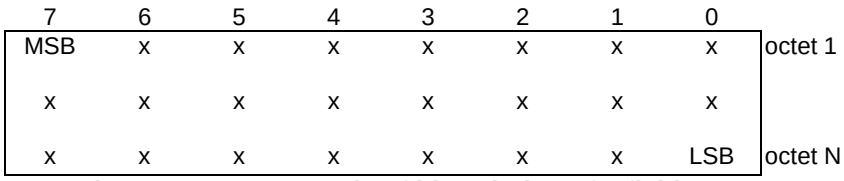


**Figure 7.1.1-1: Example of bit ordering of a field**

### 7.1.2 Message types of FTT-IMS messages

#### 7.1.2.1 Generic FTT-IMS envelope

Generic FTT-IMS envelope defines structure of messages passed via FTT-IMS.

Generic FTT-IMS envelope is coded according to figure 7.1.2.1-1 and table 7.1.2.1-1.

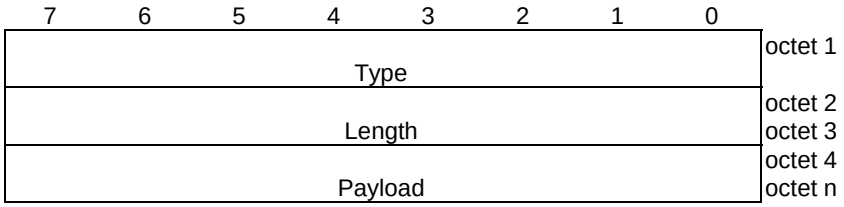


**Figure 7.1.2.1-1: Generic FTT-IMS envelope**

**Table 7.1.2.1-1: Generic FTT-IMS envelope**

| |
|---|
| Type field indicates the envelope type.<br><br>Length field indicates the length of the generic FTT-IMS envelope in octets.<br><br>Payload field is an optional field and its value depends on the envelope type. |

#### 7.1.2.2 IP packet envelope

IP packet envelope is coded according to figure 7.1.2.2-1 and table 7.1.2.2-1.

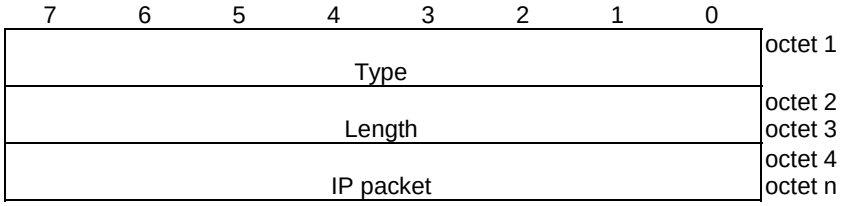


**Figure 7.1.2.2-1: IP packet envelope**

**Table 7.1.2.2-1: IP packet envelope**

| |
|---|
| Type field is according to subclause 7.1.2.1 and is set to 1.<br><br>Length field is according to subclause 7.1.2.1. The Length field value is bigger than 3.<br><br>IP packet field contains an IPv4 packet according to IETF RFC 791 [5] or IPv6 packet according to IETF RFC 2460 [7]. |

# Annex A (informative): Change history

| Change history | | | | | | |
|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2013-08 | CT1#84 | C1-133160 | | | Skeleton of TS from rapporteur | | 0.0.0 |
| 2013-08 | CT1#84 | C1-133161<br>C1-133157 | | | Incorporate agreed P-CRs from CT1#84 | 0.0.0 | 0.1.0 |
| 2013-10 | CT1#84bis | C1-134105<br>C1-134445 | | | Incorporate agreed P-CRs from CT1#84bis | 0.1.0 | 0.2.0 |
| 2013-12 | CT-62 | CP-130718 | | | Version 1.0.0 created for presentation to CT62 for information | 0.2.0 | 1.0.0 |
| 2014-01 | CT1#86 | C1-140019 | | | Minor corrections | 1.0.0 | 1.1.0 |
| 2014-02 | CT-63 | CP-140111 | | | Version 2.0.0 created for presentation to CT-63 for approval | 1.1.0 | 2.0.0 |
| 2014-03 | Post CT-63 | | | | Version 12.0.0 created after approval at CT-63 | 2.0.0 | 12.0.0 |
| 2014-06 | CT-64 | CP-140332 | 0001 | | Editorial corrections | 12.0.0 | 12.1.0 |
| 2015-06 | CT-68 | CP-150329 | 0002 | | Aligning TLS profiles used by CT1 specifications with SA3 agreed TLS profile | 12.1.0 | 13.0.0 |

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-03 | CT-75 | | | | | Upgrade to Rel-14 | 14.0.0 |
| 2018-06 | SA-80 | - | - | - | | Update to Rel-15 version (MCC) | 15.0.0 |

# History

| Document history | | |
|---|---|---|
| V15.0.0 | June 2018 | Publication |
| | | |
| | | |
| | | |
| | | |