ETSI TS 103 756 V1.1.1 (2021-11)

TECHNICAL SPECIFICATION

Emergency Communications (EMTEL); PEMEA Instant Message Extension

Reference

DTS/EMTEL-00053

Keywords

application, emergency

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

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.

Executive summary

The Pan-European Mobile Emergency Application (PEMEA) architecture provides a framework to enable applications supporting emergency calling functionality to contact emergency services while roaming. PEMEA caters for a range of extension capabilities, including Instant Messaging (IM) which provides a text-based chat capability between the App user and the PSAP. The present document provides a specification for an IM capability for PEMEA.

Introduction

Instant Message (IM) is commonly referred to as chat and the two terms are used interchangeably in the present document.

The document assumes a working knowledge of PEMEA and familiarity with the PEMEA specification ETSI TS 103 478 [1]. Terms common to the PEMEA specification are not redefined or explained in detail in the present document.

1 Scope

The present document describes the PEMEA Instant Message capability for PEMEA and the need for this functionality. The required entities and actors are identified along with the protocol, specifying message exchanges between entities. The message formats are specified and procedural descriptions of expected behaviours under different conditions are detailed.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 478 (V1.2.1): "Emergency Communications (EMTEL); Pan-European Mobile Emergency Application".

[2] IANA language subtag registry.

NOTE: Available at http://www.iana.org/assignments/language-subtag-registry/language-subtag-registry.

[3] IETF RFC 2617: "HTTP Authentication Basic Digest Access Authentication", June 1999.

[4] IETF RFC 6750: "The Oauth 2.0 Authorization Framework: Bearer Token Usage", October 2012.

[5] PEMEA Instant Message JSON Schema forge repository.

NOTE: Available at https://forge.etsi.org/rep/emtel/ts-103-756/json-schema.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IETF RFC 6753: "A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)", October 2012.

[i.2] Open Mobile Alliance OMA-TS-MLP-V3-2-20110719-A: "Mobile Location Protocol 3.2" July 2011.

[i.3] Open Mobile Alliance OMA-TS-MLP-V3-3-1-20111117-A: "Mobile Location Protocol 3.3.1", November 2011.

[i.4] Open Mobile Alliance OMA-TS-MLP-V3-4-20150512-A: "Mobile Location Protocol 3.4", May 2015.

[i.5] IETF RFC 7519: "JSON Web Token (JWT)", May 2015.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

security: techniques and methods used to ensure:

- **authentication** of entities accessing resources or data;
- **authorization** of authenticated entities prior to accessing or obtaining resources and/or data;
- **privacy** of user data ensuring access only to authenticated and authorized entities;
- **secrecy** of information transferred between two authenticated and authorized entities.

trusted: identity of entity assured through an approved authentication mechanism and the entity authorized to perform the action

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Application Provider
App	Application
EDS	Emergency Data Send (message)
ETSI	European Telecommunications Standards Institute
HELD	HTTP-Enabled Location Delivery
HTTP	Hyper-Text Transfer Protocol
IETF	Internet Engineering Task Force
IM	Instant Messenger
JSON	JavaScript Object Notation
MLP	Mobile Location Protocol
Pa	PEMEA Application to AP interface
PEMEA	Pan-European Mobile Emergency Application
PIM	PSAP Interface Module
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
SIP	Session Initiation Protocol
SIPS	SIP Secure
TLS	Transport Layer Security
tPSP	terminating PSP
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time

4 PEMEA capability extensions

4.1 Overview of extension in PEMEA

PEMEA extension capabilities are defined in ETSI TS 103 478 [1] and are implemented through the use of "reach-back" URIs. The Application Provider (AP) node advertises capabilities as part of the initial forward message through the network, the Emergency Data Send (EDS) message, and the terminating PSAP Service Provider (PSP) or PSAP responds with a the subset of capabilities that it supports, thus binding the emergency session between the AP and the terminating emergency node.

Specifically, the capabilities are sent as information elements in the apMoreInformation element of the EDS message. The information element and apMoreInformation structures are defined in clauses 10.3.11 and 10.3.12 of ETSI TS 103 478 [1]. An information element in a PEMEA EDS message identifies a capability and each capability is made up of three distinct parts:

- typeOfInfo: what function does the information element serve;
- protocol: the specific semantics for using the function;
- value: the URI through which the service is invoked.

Table 10 in ETSI TS 103 478 [1] identifies an initial set of "typeOfInfo" values used to specify a range of capability extensions for PEMEA. However, beyond the Location_Update and SIP_Request values described in Table 11 of ETSI TS 103 478 [1], protocols are left for further study and definition in subsequent specifications such as the present document.

4.2 Service support indication and response

4.2.1 Service definition

ETSI TS 103 478 [1] defines the instant message, "IM", typeOfInfo in Table 10, but does not elaborate further on protocols in Table 11. The present document provides a concrete definition of the "IM" typeOfInfo in PEMEA through the specification of a protocol value.

Table 1: Extended AP Information Type Protocol Registry

Info type Value	Protocol Token	Description
Location_Update	HELD_Deref	Location requested using a HELD location request per the HELD de-reference specification [i.1].
	MLP_3.2	Mobile Location Protocol Version 3.2 [i.2]
	MLP_3.3	Mobile Location Protocol Version 3.3 [i.3].
	MLP_3.4	Mobile Location Protocol Version 3.4 [i.4].
SIP_Request	sip	Requesting a PSAP/PSP SIP URI to which the device can send an INVITE.
	sips	Requesting a PSAP/PSP SIPS URI to which the device can send an INVITE.
IM	PEMEA	Instant Messaging functionality is supported using the PEMEA message exchange protocol.
NOTE: The PEMEA message exchange protocol is specified in clause 6 of the present document.		

4.2.2 Service support indication

AP needing to indicate that the Application it is serving can support instant messaging using the PEMEA protocol would include the following information element in the apMoreInformation element of the EDS associated with the emergency session:

```
<information typeOfInfo="IM" protocol="PEMEA">
    https://ap.example.pemea.help/48sne8aopaop
</information>
```

4.2.3 Service support response

A terminating node that can support the "IM" "PEMEA" capability includes this capability in the apMoreInformation element returned to the AP in the onCapSupportPost. This is described in clause 11.1.4 of ETSI TS 103 478 [1] with the value for "IM" "PEMEA" provided in the example below.

```
<apMoreInformation xmlns="urn:pemea:apps:xml:ns:pemea:base">
    <information typeOfInfo="IM" protocol="PEMEA"/>
</apMoreInformation>
```

5 Security

5.1 Transport security

The chat-room service is identified to potential room participants as an HTTPS URI. The connection is made using TLS 1.3 but may be made using TLS 1.2 but shall not fallback below TLS 1.2. The connecting participant shall authenticate to the chat-room service using domain certificates and a Bearer token [4]. Once the connecting entity is authenticated and authorization granted the connection is upgraded to a websocket. The websocket is expected to remain open while the entity is "online". The protocol is resilient to connections being dropped, so an entity may reconnect as long as the EDS session remains active in the PSAP.

The lists for the TLS 1.3 and TLS 1.2 acceptable cipher suites are included in annex B. These lists are informative and are based on best information at the time of writing. Older cipher suites not included in either of these lists shall not be used.

5.2 Security token usage

The HTTP Authorization header field is defined in IETF RFC 2617 [3] and it specifies that the usage is a scheme followed by a value, where the value may have a structure, as is the case for the digest authentication scheme.

Security token usage in the HTTP Authorization header field was originally specified for use with OAuth and is defined in IETF RFC 6750 [4]. Here the use of the OAuth "Bearer token" is specified so the scheme of the Authorization header field is Bearer, following the scheme a token is placed. The token is a base64 encoded string.

Token usage in the IM PEMEA specification follows the Bearer scheme defined in IETF RFC 6750 [4].

Tokens issued by entities in the IM PEMEA architecture are expected also to be the validating entities, or to have ties to the validating entities, consequently, whether the tokens are opaque or follow a convention such as JSON Web Token (JWT) [i.5] is not considered relevant to usage and is not specified further.

IETF RFC 6750 [4] mandates the usage of TLS for use with Bearer tokens, this usage is further defined in clause 5.1 of the present document.

6 Procedures and signalling

6.1 Service invocation

6.1.1 Service invocation procedures

Once the terminating PSP or PSAP has responded to the AP that it can support the PEMEA IM service then the AP shall be capable of accepting a service invocation on the provided URI at any time. The AP shall only accept an IM service invocation from the PIM or tPSP that sent the onCapSupportPost message.

The PSAP invokes the IM service by:

a) The call-taker initiating their willingness to chat to the PSAP Interface Module (PIM) in the PSAP or the tPSP.

b) The PIM/tPSP requesting the chat server create a chat-room.

c) The chat server creating a chat-room and return a URI to the PIM/tPSP.

d) The PIM/tPSP obtains Bearer token for the call-taker and AP.

e) The PIM/tPSP returns the URI and Bearer token to the PSAP call-taker.

f) The call-taker connects to the chat-room authenticating using the Bearer token.

g) The PIM/tPSP calling the URI provided by the AP for the IM-PEMEA service and including the URI for the chat-room and a Bearer token in this invocation. Note that the URI is the same for the call-taker and the caller, but the Bearer tokens are different.

h) The AP indicates to the App that the PSAP wishes to chat with the user.

i) The user indicates their willingness to chat with the PSAP to AP.

j) The AP initiates a connection to the chat-room authenticating using the Bearer token.

It is important to note that it is always the AP that authenticates to the chat room and consequently all messages from the App shall traverse the AP. The present document only defines the protocol between the AP and other trusted entities e.g. PSAP call-taker or First Responder, and the chat-room in the PSAP, it does not define the chat Pa messaging between the App and the AP.

6.1.2 Service invocation object

The PIM/tPSP invokes the IM service in the AP by posting to the URI provided in the IM information element included in the apMoreInformation contained in the EDS. The POST message includes a body containing a JSON object. The JSON object provides the chat room URI as well as indicates how the AP should authenticate itself to the chat room.

Table 2: Invocation object fields

Element Name	Presence	Description
uri	Mandatory	The URI of the chat room.
token	Mandatory	A security token used to authenticate the AP to the chat room. The AP shall include the token in the HTTP Authorization header using the Bearer token scheme. The AP shall use the token each time it needs to establish or re-establish a connection to the chat room for the duration of the App emergency session. The AP shall not provide the token to the App.
expiry	Mandatory	Specifies the expiry time of the security token. expiry is an integer specifying the number of second since UTC epoch, 00:00:00 1st of January 1970.

Invocation example:

```
{
    "uri": "https://chat-server.example.com/room/534wafds21s21fdf",
    "token": "PPtzs5zzG5Pkf61KPz51",
    "expiry": "1590563357576"
}
```

6.2 Chat-room creation and deletion

The chat-room is created by the chat-server under direction of the PSAP call-taker via the PIM or tPSP. When the chat-room is created, a logging function shall be created with it to scribe all messages into and out of the chat-room. The chat-room may also contain a chat-bot that is used to invoke services, such as translation services when required. The chat-bot does appear as a user in the USER_LIST as its role is indicated as TRANSLATOR. This flow is shown in Figure 1.

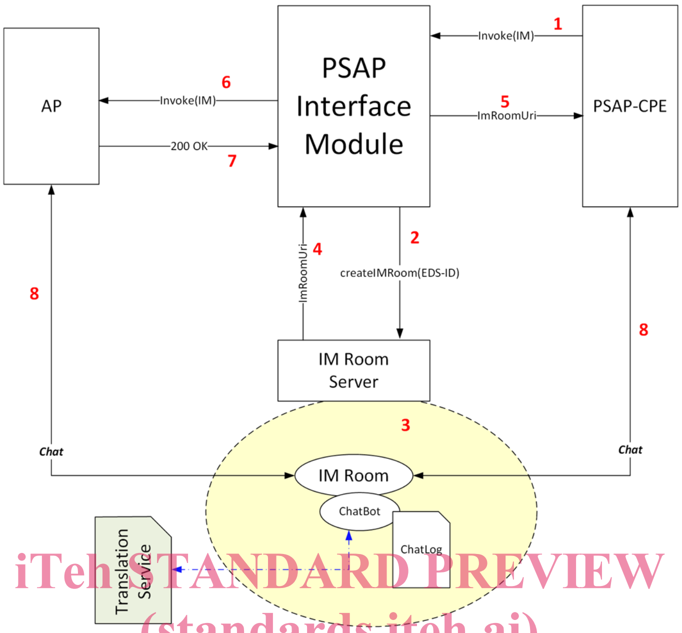

Figure 1: Chat initiation

Once the chat-room is created it remains active as long as the PIM or tPSP maintains a context for the EDS. When EDS context is deleted the chat-room is also destroyed.

6.3 Chat-room creation, JOIN, and ERROR signalling

6.3.1 Semantics

The figure in the following sub clauses show the signalling involved in establishing and subsequently joining a PEMEA chat session. By necessity the diagrams show four distinctive types of signalling:

- Semantic signalling across the Pa interface between the App and the AP is explicitly not defined in PEMEA. So, while the message names and contents may not align with any specific implementation, the semantics of what the messages convey should be understood.
- Core PEMEA signalling are explicit messages defined in the PEMEA technical specification ETSI TS 103 478 [1].
- Chat semantic signalling is messaging that needs to occur between the PSAP call-taker equipment, the PIM/tPSP and the software entities and components required to establish the chat service. These messages are intended to provide an idea of what needs to occur, not how it should be implement. Consequently, they are informative only and not normative.
- IM (chat) normative signalling messages and semantics explicitly defined in the present document.