ETSI TS 103 871 V1.1.1 (2022-12)

TECHNICAL SPECIFICATION

Emergency Communications (EMTEL); PEMEA Real-Time Text Extension

Reference

DTS/EMTEL-00064

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

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 Real-Time Text (RTT) which provides a text-based character by character exchange capability between the App user and the PSAP. The present document provides a specification for an RTT capability for PEMEA.

Introduction

Real-Time Text (RTT) communications are used extensively by people with hearing and speech disabilities around the world. These systems convey letters as they are typed from the source to the destination. The International Telecommunications Union (ITU) defines clear guidelines for what is required to support RTT. The present document defines an RTT protocol, complying with ITU guidelines, for use in the Pan-European Mobile Emergency Application (PEMEA) framework.

The present document does not preclude PEMEA from being used to support and initiate other RTT protocols or implementations.

The present 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 Real-Time Text (RTT) capability, 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: "Emergency Communications (EMTEL); Pan-European Mobile Emergency Application".

[2] ETSI TS 103 756: "Emergency Communications (EMTEL); PEMEA Instant Message Extension".

[3] Recommendation ITU-T T.140: "Protocol for multimedia application text conversation".

[4] IANA language subtag registry.

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

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

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

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 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: As defined in ETSI TS 103 478 [1].

3.2 Symbols

Void.

3.3 Abbreviations

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

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AESGCM	Advanced Encryption Standard key used with GCM
AP	Application Provider
App	Application
BEL	audible Bell sound
BS	Back Space
CPE	Customer Premises Equipment
CR	Carriage Return
DHE	Diffie-Hellman key Exchange
ECDHE	Elliptic-Curve Diffie-Hellman key Exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
EDS	Emergency Data Send (message)
ESC	Escape
ETSI	European Telecommunications Standards Institute
GCM	Galios/Counter Mode
HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure HTTP
IANA	Internet Assigned Numbers Authority
ID	IDentifier
IETF	Internet Engineering Task Force
INT	Interrupt character
ITU	International Telecommunications Union
JSON	JavaScript Object Notation
JWT	JSON Web Token
LF	Line Feed
MAC	Message Authentication Code
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
RSA	Rivest Shamir Aldeman public key encryption algorithm

RTT	Real-Time Text
SGR	Select Graphic Rendition
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SOS	Start Of String
ST	String Terminator
TLS	Transport Layer Security
tPSP	terminating PSP
UCS	Universal Multiple-Octet Coded Character Set
URI	Uniform Resource Identifier
UTC	Coordinated Universal Timer
UTF-8	UCS Transformation Format (8 bit words)

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 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. ETSI TS 103 756 [2] describes the concrete specification for PEMEA Instant Message protocol.

4.2 Service support indication and response

4.2.1 Service definition

ETSI TS 103 478 [1] defines the Real-Time Text, "RTT", typeOfInfo in Table 10, but does not elaborate further on protocols in Table 11. The present document provides a concrete definition of the "RTT" typeOfInfo in PEMEA through the present document of a protocol value. The definition in Table 1 shall be considered as an extension to Table 11 in ETSI TS 103 478 [1].

Table 1: Extended AP Information Type Protocol Registry

Info type Value	Protocol Token	Description
RTT	PEMEA	Real-Time Text functionality is supported using the PEMEA message exchange protocol

4.2.2 Service support indication

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

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

4.2.3 Service support response

A terminating node that can support the "RTT" "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 "RTT" "PEMEA" provided in the example below:

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

4.2.4 Auto response service

The original intent of many emergency applications was to provide ancillary data to the PSAP that was associated with an emergency voice call that the PSAP had, or soon would, receive. As a consequence, a PIM or tPSP usually notifies the PSAP-CPE when an EDS has arrived, but does not respond to the AP until a PSAP call-taker has answered the call. Operating in this manner allows for smart routing solutions ensuring that only the PSAP with the call binds the PEMEA session to the AP, ensuring that the data is always available to the call-taker rather than it being missing because it went to the wrong PSAP.

ETSI TS 103 478 [1] identifies some types of capabilities, most notably the SIP_Request capabilities, as being responded to automatically, that is, the PIM or tPSP sends an immediate onCapSupportPost message with all supported capabilities if the EDS contains a SIP_Request capability. This functionality is described in clause 8 of ETSI TS 103 478 [1] and came about because there was no way for the App to make a voice call until it has a destination SIP URI, so there was no possible way for the data to not be available at the destination PSAP.

Another reason for auto-response is that no conventional carrier/mobile voice call will be placed as part of the emergency communication. That is, only PEMEA advanced services will be used for communicating between the caller and the PSAP call-taker.

The PEMEA RTT capability falls into this latter category of services, that is, it is used in place of a conventional carrier/mobile voice call. Consequently, a PSAP (PIM or tPSP) supporting this capability and with the capacity to handle the communication shall respond to the AP with an onCapSupportPost message immediately on receipt of an EDS containing a RTT PEMEA capability. The onCapSupportPost message shall contain the RTT PEMEA capability along with any other capabilities that the PSAP supports.

If the PSAP does not have the ability or capacity to support the request then it may forward the request to a neighbouring PSAP with whom it has an agreement to do so. In this situation the original PSAP shall not send an onCapSupportPost message to the originating AP. If, having forwarded the EDS, the PSAP receives an error from the destination PSAP then the originating PSAP shall send an onErrorPost event to the AP including the cause of the error.

5 Mapping to T.140

5.1 T.140 special character support

Recommendation ITU-T T.140 [3] defines requirements and procedures for RTT systems. For the most part these are mapped directly. With the movement to modern communications system however, some of the requirements in Recommendation ITU-T T.140 [3] are no longer relevant. In other cases, functionality is not provided as it is available through other PEMEA extensions or is supported implicitly through the protocol itself rather than through special characters. Table 2 indicates which functionality from clause 7 of Recommendation ITU-T T.140 [3] is supported and how.

Table 2: PEMEA RTT support for T.140 special characters

Name	Supported	Description
BEL	No	No alerting in in the communication is provided
BS	Yes	Backspace character is sent as 0x08, converted to UTF-8, inside a TEXT_MESSAGE
NEW LINE	Yes	New line character is sent as 0x0A, converted to UTF-8, inside a TEXT_MESSAGE
CR LF	No	No-standard and non-preferred, not supported
INT	No	No mode negotiation is required
SGR	No	Not supported
SOS	No	Not supported
ST	No	Not supported
ESC	Yes	The present document supports the sending and receiving of the ESC (0x1B) control character, however, rendering, displaying and interpretation of control sequences is not specified
Byte order mark	No	Synchronization is not required via a Web Socket

The protocol described in the present document addresses the establishment of connections, disconnections and the transfer of data between entities, it does not attempt to address the display requirements of Recommendation ITU-T T.140 [3]. However, the intention from T.140 Appendix I shall be fulfilled. "*The display of text from the members of the conversation should be arranged so that the text from each participant is clearly readable, and its source and the relative timing of entered text is visualized in the display. Mechanisms for looking back in the contents from the current session should be provided. The text should be displayed as soon as it is received*".

All text is transferred using UTF-8 which can represent most language character sets. The language that the user intends to communicate with is provided in the JOIN message, see clause 8.3. The language shall be specified using one of the languages provided in the language sub-tags registered with IANA [4]. The present document does not provide guidance on whether multi-lingual session participants may switch languages during the session or not though the general recommendation is against taking this action.

Text messages consist of one or more characters. Characters are transferred from the App to the AP either in real-time, as they are typed, or in batches at 0,5 second intervals so that a character is always transferred within 0,5 seconds of having been typed. This functionality is described in clause 6.1.1 of Recommendation ITU-T T.140 [3].

5.2 ESC character sequence support

ESC character sequences in the present document are a set of characters bounded by ESC characters (0x1B) on either side. For example 0x1B:)0x1B may display a smiley face. The present document does not define any ESC character sequences nor does it provide any guidance on rendering or interpretation beyond all characters between two ESC characters forming the escape sequence.

An entity shall ignore all escape sequence characters if an explicit escape sequence code set has not been established through some other means. The present document leaves the possibility open for a future revision of the present document to define common sets of escape sequences.

The ESC sequence, open ESC character, intermediate characters and closing ESC character shall be sent in a single message and the receiver receiving a single erase character shall erase any and all characters in the ESC sequence.

Any message containing a partial ESC sequence shall be ignored.

6 Security

6.1 Transport security

The RTT 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 RTT service using a Bearer token in the HTTP Authentication header field as described in IETF RFC 6750 [6]. 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.

6.2 Security token usage

The HTTP Authorization header field is defined in IETF RFC 2617 [5] 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 [6]. 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 RTT PEMEA specification follows the Bearer scheme defined in IETF RFC 6750 [6].

Tokens issued by entities in the RTT 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) IETF RFC 7519 [i.1] is not considered relevant to usage and is not specified further.

IETF RFC 6750 [6] mandates the usage of TLS for use with Bearer tokens, this usage is further defined in clause 6.1 of the present document.

7 Procedures and signalling

7.1 Service invocation

7.1.1 Service invocation procedures

Once the terminating PSP or PSAP has responded to the AP that it can support the PEMEA RTT 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 RTT service invocation from the PIM or tPSP that sent the onCapSupportPost message.

The PSAP invokes the RTT service by:

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

b) The PIM/tPSP requesting the RTT server create an RTT-session room.

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

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

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

f) The call-taker connects to the RTT-session room authenticating using the provided Bearer token.

g) The PIM/tPSP calling the URI provided by the AP for the RTT-PEMEA service and including the URI for the RTT-session 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 communicate using RTT with the user.

i) The user indicates their willingness to communicate using RTT with the PSAP to the AP.

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