ETSI TS 104 014 V1.1.1 (2024-07)

Emergency Communications (EMTEL);
PEMEA File Exchange Extension

Reference
DTS/EMTEL-00074

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

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 File Exchange which provides a channel to exchange files between the App user and the PSAP. The present document provides a specification for a File Exchange capability for PEMEA.

Introduction

Sending and receiving files is common in most modern communication Apps. These systems allow users to upload and download files in dedicated sessions by using file servers. The present document defines a File Exchange protocol for use in the Pan-European Mobile Emergency Application (PEMEA) framework.

PEMEA File Exchange extension allows PEMEA Apps and PSAPs to exchange files, enabling PSAPs to request photos or videos from the scene that the caller records during the emergency communication. It also allows PSAPs to send files with instructions when it is needed, for example during a multi-case incident where they are receiving a large number of calls.

The specification in the present document does not preclude PEMEA from being used to support and initiate other 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 defines the PEMEA File Exchange (PFE) 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] IETF RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[3] IETF RFC 6750 (October 2012): "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[4] IETF RFC 6838 (January 2013): "Media Type Specifications and Registration Procedures".

[5] IETF RFC 7578 (July 2015): "Returning Values from Forms: multipart/form-data".

[6] IETF RFC 8089 (February 2017): "The "file" URI Scheme".

[7] IETF RFC 9110 (June 2022): "HTTP Semantics".

[8] IETF RFC 9112 (June 2022): "HTTP/1.1".

[9] ISO 8601-1:2019: "Date and time - Representations for information interchange - Part 1: Basic rules".

[10] WHATWG: "HTML Living Standard".

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

[i.2] ETSI TS 103 871: "Emergency Communications (EMTEL); PEMEA Real-Time Text Extension".

[i.3] ETSI TS 103 945: "Emergency Communications (EMTEL); PEMEA Audio Video Extension".

[i.4] IETF RFC 7519 (May 2015): "JSON Web Token (JWT)".

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** is used 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
CPE	Customer Premises Equipment
DHE	Diffie-Hellman key Exchange
ECDHE	Elliptic-Curve Diffie-Hellman key Exchange
EDS	Emergency Data Send (message)
GCM	Galois/Counter Mode
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JWT	JSON Web Token
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions
OAuth	Open Authorization
Pa	PEMEA Application to AP interface
PEMEA	Pan-European Mobile Emergency Application
PFE	PEMEA File Exchange
PIM	PSAP Interface Module
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
RFC	Request For Comments
RSA	Rivest Shamir Adleman public key encryption algorithm
SSE	Server-Sent Events
TLS	Transport Layer Security

TS	Technical Specification
tPSP	terminating PSP
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
UTF-8	8-bit Unicode Transformation Format
WHATWG	Web Hypertext Application Technology Working Group

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 the subset of capabilities that it supports, thus binding the emergency session between the AP and the terminating PSP or PSAP 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 [i.1] defines the concrete specification for PEMEA Instant Message protocol, ETSI TS 103 871 [i.2] defines the concrete specification for PEMEA Real-Time Text and ETSI TS 103 945 [i.3] defines the concrete specification for PEMEA Audio Video.

4.2 Service support indication and response

4.2.1 Service definition

The present document provides a concrete definition of the "File_Exchange" 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
File_Exchange	PEMEA	File exchange functionality is supported using the PFE protocol

4.2.2 Service support indication

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

```
<information typeOfInfo="File_Exchange" protocol="PEMEA">
    https://ap.example.pemea.help/37agq1cyusbo
</information>
```

4.2.3 Service support response

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

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

5 Architecture

5.1 Overview

The PEMEA File Exchange (PFE) capability defines a protocol to exchange files between Apps and PSAPs with a PEMEA emergency request. In order to exchange the files, a file server is needed, and the present document defines all the interfaces and procedures that the file server shall provide. This also helps to understand explicitly what is normatively specified in the present document, what is semantic, and what is normatively referred to from the present document but normatively specified in other documents.

The PFE capability was realized with disability usage in mind and the usage model for this necessitates multi-party communications where the Caller and the PSAP Call-Taker represent two parties, but other third-party user may also participate in the emergency session.

Where the procedures described in clause 5 refer to the PSAP Interface Module (PIM) PEMEA node, they may be performed by a terminating PSP or by a PIM depending on architectural decisions in PSAP infrastructure according to ETSI TS 103 478 [1].

References in clause 5 to the App may be made by Apps directly or by an App server acting as a proxy. Whether there are Apps directly connected to the AP or there is an App server connected to the AP is beyond the scope of the present document and depends on the implementation details. The File Exchange Server shall accept requests from any source as long as they are made with the authentication token that was delivered to the AP node as described in clause 0 and following all security procedures described in clause 6.

5.2 Architecture and high-level flows

PEMEA is structured around the AP being the gateway between the App and the PSAP. This model requires communications to occur, first between the App and the AP over the proprietary Pa interface and then between the AP and the associated PSAP service using the protocol mechanisms defined in the specific extension capability document, such as the present document or other PEMEA extension documents, e.g. ETSI TS 103 756 [i.1], ETSI TS 103 871 [i.2], ETSI TS 103 945 [i.3] or any other related one. For most services, this approach is fine, however, exchanging files requires high bandwidth, thus this approach may need to be relaxed somewhat to ensure that the capability delivers the required functionality. Therefore, the present document does not require that all requests to the File Exchange Server are done from the AP node, Apps can make requests to the File Exchange Server directly once they have received the URI and the token from the AP.

The present document does not explicitly define the security measures that shall be taken at the File Exchange Server to detect malicious files, but it is highly recommended that all files uploaded to the File Exchange Server are analysed with malware detection software.

Figure 1 depicts the PFE service architecture. It includes a malware detection software that is not mandatory but highly recommended.

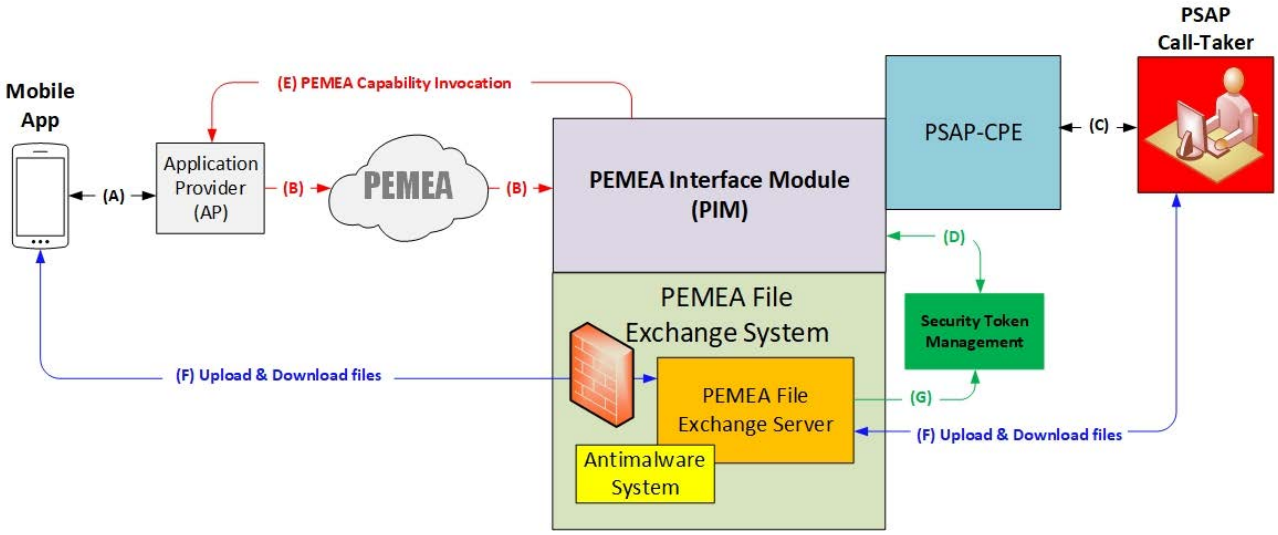

Figure 1: File Exchange architecture for PEMEA

A. Pa interface, the application makes a call to the AP indicating the PFE capability. Invocation information is returned to the App over this interface too.

B. The AP packages the information from the App into an EDS message and sends it into the PEMEA network via the Ps interface. The EDS arrives at the PIM over the Pp interface. The PIM sends an onCapSupportPost message to the AP binding the connection between the AP and the PIM.

C. The PIM notifies the PSAP-CPE which in turn notifies the PSAP Call-Taker. The call is answered and controlled by the PSAP Call-Taker over this interface also. This includes requesting the creation of a PFE session. The PSAP Call-Taker is also able to request connection credentials for additional participants over this interface.

D. On direction from the PSAP Call-Taker the PIM creates a new PFE session and requests Bearer tokens from the Security Token Management system. It shall generate at least a token for the PSAP Call-Taker and a token for the Caller.

E. The PIM invokes the PFE capability in the AP passing the URI for the PFE session as well as the Bearer token required to access it. Similar information is provided to the PSAP Call-Taker's application. The AP then passes the received information down to the App.

F. The App and the PSAP Call-Taker can make requests to the File Exchange Server using the PFE session URI and passing in their respective security tokens. Upload and download of files occurs over this interface. It is highly recommended that files received through this interface are scanned with anti-malware systems to prevent malicious files from being uploaded.

G. The File Exchange Server verifies the Bearer tokens with the Security token management system before accepting requests from the participants.

Whilst the division of the File Exchange Server in these sub-components does not need to be strictly followed, the notion of a signalling component and a media or streaming component are important for traffic path differentiation.