ETSI TS 103 478 V1.1.1 (2018-03)

Emergency Communications (EMTEL);
Pan-European Mobile Emergency Application

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5489e70-27cf-4b6a-9853-5fc3333a9667/etsi-ts-103-478-v1.1.1-2018-03

Reference
DTS/EMTEL-00036

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4f8e70-2f-cf-4f0-9853-f6333...-1103-478-v1.1.1-2018-03

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.
All rights reserved.

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 protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 6

Foreword 6

Modal verbs terminology 6

Executive summary 6

Introduction 6

1 Scope 8

2 References 8
2.1 Normative references 8
2.2 Informative references 9

3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 10

4 PEMEA architecture and functional entities 11
4.1 Introduction 11
4.2 Functional entities overview 11
4.2.1 Application (App) 11
4.2.2 Application Provider (AP) 11
4.2.3 PSAP Service Provider (PSP) 12
4.2.4 Aggregating Service Provider (ASP) 12
4.3 Interface definitions 12
4.3.1 Application Interface (Pa) 12
4.3.2 Application Provider to PSAP Service Provider Interface (Ps) 12
4.3.3 PSAP Service Provider Interface to Aggregating Service Provider Interface (Pr) 12
4.3.4 PSAP Service Provider to PSAP Interface (Pp) 13

5 PEMEA functional entity requirements 13
5.1 Introduction 13
5.2 Application requirements 13
5.3 Application provider requirements 14
5.4 PSAP service provider requirements 14
5.5 Aggregating service provider requirements 14

6 PEMEA Message Element Definitions 15
6.1 Introduction 15
6.2 emergencyDataSend Information Elements 16
6.3 emergencyDataReceived Information Elements 17
6.4 error Information Elements 17
6.5 PEMEA Confirmation Messages 17

7 PEMEA Message Flows 17
7.1 Introduction 17
7.2 Ps message flows 18
7.2.1 Ps message flow description 18
7.2.2 Ps basic flow 18
7.2.3 Ps error flow 19
7.2.4 Ps routing flow 20
7.3 Pr message flows 21
7.3.1 Pr message flow description 21
7.3.2 Pr terminating-PSP basic flow 21
7.3.3 Pr error flow 22
7.3.4 Pr end to end routing flow 23

8 PEMEA alignment with ETSI TS 103 479 25
8.1 General alignment 25
8.2 PEMEA to border control function 25

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-27cf-4464-9853-5fc3333a9667/etsi-ts-103-478-v1.1.1-2018-03

8.3 PEMEA to Legacy Network Gateway 27
9 Message transportation and processing 28
9.1 HTTP usage 28
9.2 Authenticating and authorizing PEMEA entities 29
9.3 PEMEA Securing a PSAP Retrieving Data By Reference or a reach-back URI 29
9.4 PEMEA XML Processing Rules 30
10 PEMEA XML structures and messages 30
10.1 Ps Introduction 30
10.2 Timestamps 30
10.3 General types 31
10.3.1 pemea:posIntType 31
10.3.2 pemea:nodeType 31
10.3.3 pemea:hopsType 31
10.3.4 pemea:routeType 31
10.3.5 pemea:destinationType 32
10.3.6 pemea:destinationNodeType 32
10.3.7 pemea:deliveryType 32
10.3.8 pemea:typeOfCallerIdType 32
10.3.9 pemea:callerIdType 33
10.3.10 pemea:callerIdListType 33
10.3.11 pemea:informationType 33
10.3.12 pemea:apMoreInfoType 34
10.3.13 pemea:accessDataType 35
10.3.13.1 pemea:accessDataType structure 35
10.3.13.2 network 35
10.3.13.3 wifi 35
10.3.14 pemea:accessData 36
10.3.15 pemea:msgInfoType 36
11 PEMEA Message Definition 36
11.1 emergencyDataSend Message 36
11.1.1 emergencyDataSend message structure 36
11.1.2 emergencyDataSend example 38
11.1.3 onErrorPost usage details 39
11.1.4 onCapSupportPost usage details 40
11.2 emergencyDataReceived message 41
11.2.1 emergencyDataReceived message structure 41
11.2.2 emergencyDataReceived example 42
11.3 error message 42
12 PEMEA PIDF-LO Profiling 43
12.1 Rationale 43
12.2 entity 44
12.3 tuple 44
12.4 status 44
12.5 geopriv 44
12.5.1 geopriv element profile 44
12.5.2 location-info 44
12.5.2.1 location-info profile 44
12.5.2.2 Confidence 45
12.5.3 usage-rules 45
12.5.4 method 46
12.5.5 provided-by 46
12.6 timestamp 46
12.7 PIDF-LO example 46
13 PEMEA Additional-Data Profiling 46
13.1 Rationale 46
13.2 Additional-Data :- provided-by 47
13.3 EmergencyCallDataValue 47
13.4 EmergencyCallData.ProviderInfo 47
13.4.1 EmergencyCallData.ProviderInfo profile 47

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-27cf-4a6a-9853-5fc3333a9667/etsi-ts-103-478-v1.1.1-2018-03

13.4.2 DataProviderContact :- vcard 48
13.4.2.1 DataProviderContact :- vcard profile 48
13.4.2.2 DataProviderContact :- org 48
13.4.2.3 DataProviderContact :- adr 49
13.4.2.4 DataProviderContact :- email 50
13.4.2.5 DataProviderContact :- URL 50
13.4.3 EmergencyCallData.ProviderInfo:- Complete Example 50
13.5 EmergencyCallData.DeviceInfo 51
13.6 EmergencyCallData.SubscriberData 51
13.6.1 EmergencyCallData.SubscriberData profile 51
13.6.2 SubscriberData :- vcard 52
13.6.2.1 SubscriberData :- vcard profile 52
13.6.2.2 SubscriberData :- Caller's name 52
13.6.2.3 SubscriberData :- home address 53
13.6.2.4 SubscriberData :- language 54
13.6.2.5 SubscriberData :- gender 54
13.6.2.6 SubscriberData :- bday 54
13.6.2.7 SubscriberData :- tel 55
13.6.2.8 SubscriberData :- email 56
13.6.2.9 SubscriberData :- Emergency Family Contacts 56
13.6.3 EmergencyCallData.SubscriberData :- Complete Example 57
13.7 Additional-Data :- EmergencyCallDataReference 59
13.8 provided-by : Complete Examples 59

14 Operating Procedures 60
14.1 Application Provider Operating Procedures 60
14.1.1 AP sending an EDS to the PSP 60
14.1.2 AP reach-back URI queries 61
14.1.3 Call termination (ending) and URI invalidation 62
14.2 PSAP Service Provider Operating Procedures 62
14.2.1 PSP receiving an EDS message over Ps 62
14.2.2 PSP sending an EDS message over Pr 64
14.2.3 PSP receiving an EDS message over Pr 64
14.3 Aggregating Service Provider Operating Procedures 65
14.3.1 Overview of Pr 65
14.3.2 ASP receiving an EDS message over Pr 65
14.3.3 ASP sending an EDS message over Pr 66

15 Example message Flows 67
15.1 Description 67
15.2 AP to PSP EDS 67
15.3 oPSP to AP EDR 68
15.4 oPSP to ASP EDS 68
15.5 ASP to oPSP EDR 70
15.6 ASP to tPSP EDS 70
15.7 tPSP to ASP EDR 72

16 PEMEA Schema 72

Annex A (informative): Route Determination 77

Annex B (informative): Caller Data 79

Annex C (informative): Additional AP Information 80

History 81

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5148b8e7-27cf-4b6a-9853-5fc3333a9567/etsi-ts-103-478-v1.1.1-2018-03

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 Special Committee Emergency Communications (EMTEL).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-27cf-4b6a-9453-5fc3333a9667/etsi-ts-103-478-v1.1.1-2018-03

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 the requirements and architecture for a solution to provide emergency application interconnection. It specifies the protocols and procedures enabling interoperable implementations of the architecture and provides extension points to enable new communication mechanisms as they evolve.

Introduction

The rise of smart devices such as smart phones, tablets and laptops has led to an explosion in communications applications. Many of these applications aim to supplement existing communications services, such as providing caller and location information for emergency calls, while others seek to provide alternative communication mechanisms such as total conversation and instant messaging for example. Many of these applications already exist in limited local capacities but lack a common framework for easy interconnection. This limitation prohibits a user's application operating in a region other than the one it was developed in and having his/her information and accurate location information passed to the PSAP serving their location. The Pan-European Mobile Emergency Application (PEMEA) architecture provides a solution to interconnect these applications.

The present document amalgamates the European Emergency Number Association (EENA) PEMEA Requirements and Functional Architecture document [i.2] and it companion document the PEMEA Protocol and Procedures Specification [i.3] providing a single comprehensive document detailing PEMEA.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-27cf-4b6a-9853-5fc3333a9667/etsi-ts-103-478-v1.1.1-2018-03

1 Scope

The present document is divided into two parts. The first part provides the requirements and functional architecture while the second part provides the protocol and procedures for implementing the Pan-European Mobile Emergency Application (PEMEA). The first part identifies the key functional entities involved in the emergency application architecture, the interfaces between each functional entity, and the requirements on each interface. The second part defines the data exchanges, message, protocols and procedures used across each of the identified PEMEA interfaces.

It is recognized that many existing application implementations combine the functional entities identified in the present document into a single entity. The most common example of combined functional entities is the combined Application Provider (AP) and PSAP Service Provider (PSP), these are common because it is often the PSAP that writes or engages a third-party to write a local emergency application that interfaces directly with the PSAP. The present document does not seek to disallow integrated node implementations, however, it does not define how additional applications or application providers using proprietary application programming interfaces (APIs) and protocols can provide PEMEA extended features, such solutions are left to the integrated node providers.

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] IETF RFC 2818: "HTTP Over TLS", May 2000.

[2] IETF RFC 2965: "HTTP State Management Mechanism", October 2000.

[3] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format", December 2005.

[4] IETF RFC 5491: "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", March 2009.

[5] IETF RFC 3966: "The tel URI for telephone Number", December 2004.

[6] IETF RFC 7459: "Representation of Uncertainty and Confidence in the Presence Information Data Format Location Object (PIDF-LO)", February 2015.

[7] IETF RFC 3863: "Presence Information Data Format (PIDF)", August 2004.

[8] IETF RFC 5139: "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", February 2008.

[9] IETF RFC 6848: "Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)", January 2013.

[10] IANA: "Method Token Registry of Values".

NOTE: Available at http://www.iana.org/assignments/method-tokens/method-tokens.xhtml#method-tokens-1.

[11] IETF RFC 7852: "Additional Data Related to an Emergency Call", July 2016.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548bc7b0-27cf-4b6a-9353-5f13333a4667/etsi-ts-103-478-v1.1.1-2018-03

[12] IETF RFC 7105: "Using Device-Provided Location-Related Measurements in Location Configuration Protocols", January 2014.

[13] IANA: "Language subtag registry".

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

[14] ISO 639-3 (2007): "Codes for the representation of names of languages -- Part 3: Alpha-3 code for comprehensive coverage of languages".

NOTE: Available at https://www.iso.org/standard/39534.html

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

[16] IETF RFC 5808: "Requirements for a Location-by-Reference Mechanism", May 2010.

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-27cf-4b66-9853-5fc3333a9667/etsi-ts-103-478-v1.1.1-2018-03

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 103 479: "Emergency Communications (EMTEL); Core elements for network independent access to emergency services".

[i.2] EENA: "Pan-European Mobile Emergency Application (PEMEA) Requirements and Functional Architecture", Version 7, February 2015.

NOTE: Available at http://www.eena.org/download.asp?item_id=158.

[i.3] EENA "Pan-European Mobile Emergency Application (PEMEA) Protocol and Procedures Specification", Version 5.0, April 2016.

NOTE: Available at http://www.eena.org/download.asp?item_id=175.

3 Definitions and abbreviations

3.1 Definitions

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

security: refers to 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: entity is considered trusted if its identity can be assured through authentication mechanisms described in the present document and it is recognized as authorized to access the specific resource or data based on the mechanisms defined in the present document

3.2 Abbreviations

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

AP	Application Provider
API	Application Programming Interface
App	Application
ASP	Aggregating Service Provider
BCF	Border Control Function
BSSID	Basic Service Set Identifier
CID	Cell Identifier
CPE	Customer Premises Equipment
ECRF	Emergency Call Routing Function
EDR	Emergency Data Received (message)
EDS	Emergency Data Send (message)
EENA	European Mobile Emergency Number Association
ESInet	Emergency Services IP Network
ESRP	Emergency Services Routing Proxy
ETSI	European Telecommunication Standards Institute
GML	Geography Markup Language
GNSS	Global Navigation Satellite System
HELD	HTTP-Enabled Location Delivery
HTTP	Hyper-Text Transfer Protocol
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identifier
LIF	Location Interworking Function
LIS	Location Information Server
LNG	Legacy Network Gateway
MAC	Media Access Control
MCC	Mobile Country Code
MLP	Mobile Location Protocol
MNC	Mobile Network Code
MSISDN	Mobile Service International Subscriber Dial Number
OMA	Open Mobile Alliance
oPSP	Originating PSP
OTT	Over the Top
Pa	PEMEA Application to AP interface
PEMEA	Pan-European Mobile Emergency Application
PIDF-LO	Presence Information Data Format Location Object
Pp	PEMEA PSP to PSAP interface
Pr	PEMEA PSP to ASP or ASP to PS interface
Ps	PEMEA AP to PSP interface
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
PSTN	Public Switched Telephone Network
RTT	Real-Time Text
SIP	Session Initiation Protocol
SIPS	SIP Secure
TLS	Transport Layer Security
tPSP	terminating PSP
ttl	time to live
UCF	Universal Character Set

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-27cf-4b6a-9853-5fc333...7/etsi-ts-103-478-v1.1.1-2018-03

UMTS	Universal Mobile Telecommunication System (cellular 3G)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Universal Resource Name
UTC	Coordinated Universal Time
UTF	UCF Transformation Format
VSP	Voice Service Provider
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 PEMEA architecture and functional entities

4.1 Introduction

The extensive deployment of existing mobile emergency applications and their interconnection into a Pan-European Emergency Application ecosystem has prompted the definition of entities identified in Figure 1.

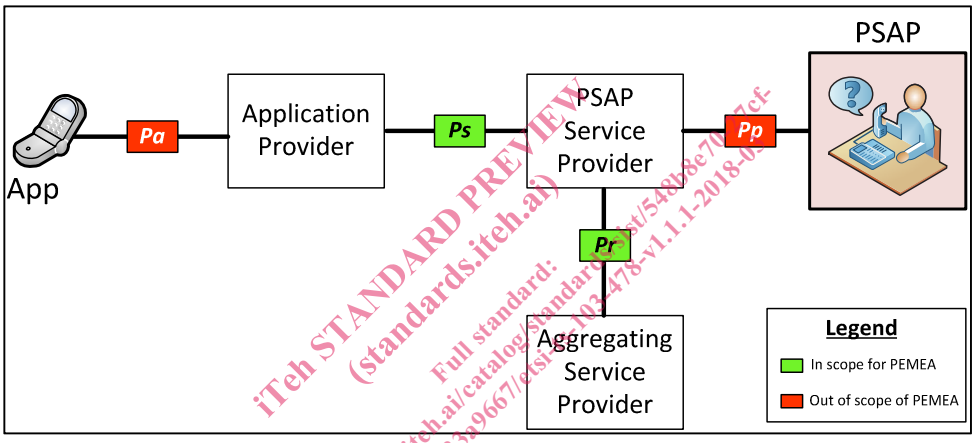

Figure 1: PEMEA Reference Architecture

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8e70-7cf-4b6a-9853-5a3333a9667/etsi-ts-103-478-v1.1.1-2018-03

In some implementations functional entities may be owned and operated by the same commercial entity, for example the Application Provider (AP) and the PSAP Service Provider (PSP) may be the same. In these cases, the external interfaces shown in the reference architecture need only apply when communicating with external entities.

4.2 Functional entities overview

4.2.1 Application (App)

Software that runs on a smartphone or mobile computing platform that is capable of making an emergency call using mobile network operator call control machinery (3G/4G/WiFi). Simultaneous to call establishment the App sends user authentication information to an Application Provider and subsequently sends location, connectivity and other information about the caller to the Application Provider for subsequent conveyance to a PSAP.

4.2.2 Application Provider (AP)

The Application Provider (AP) is the entity that provides a mobile emergency application. It is responsible for authenticating the Application user prior to accepting caller information from the App. The AP needs to format the data received from the App, possibly combining it with caller information stored in AP server, and conveying it to a PSAP Service Provider (PSP). There needs to be a trust relationship between the AP and PSP. Where the AP and PSP are not the same entity then data formats defined in the present document shall be used to convey caller information from the AP to the PSP.

In the general case, an AP has a relationship with a single PSP. However, an AP may have a relationship with more than one PSP. When this is the case it is up to the AP to determine which PSP to send the information to. How the AP makes this determination is out of scope of the present document, but the AP shall only send the information to one PSP to avoid multiple routing of the same messages through the network.

4.2.3 PSAP Service Provider (PSP)

The role of the PSAP Service Provider (PSP) is to take caller information from trusted sources and ensure that it is provided to the correct PSAP. Where the PSP directly serves the PSAP for which the information is destined, then it is referred to as the terminating-PSP (tPSP). If a PSP receives information that it knows is not for a PSAP that it directly services then it should use its knowledge of other PSPs to attempt to deliver the information to the PSP serving the correct PSAP. When this occurs it is referred to as an originating-PSP (oPSP).

Information coming from trusted sources shall comply with the data formats and communication mechanisms defined in the present document.

Trusted information may come from one of two sources. It may come directly from an AP with which the PSP has a direct trust relationship (***Ps***). Alternatively, the information may come from an AP with which the terminating-PSP has no direct trust relationship (***Pr***). In this latter case, the trust relationship is brokered by another PSP or chain of PSPs to the terminating-PSP.

How the PSP provides or renders information to a PSAP that it directly services is out of scope of the present document.

4.2.4 Aggregating Service Provider (ASP)

The primary role of the PSP is to ensure that accurate and trusted caller information is provided to the PSAP that is terminating an emergency call. A PSP may have knowledge of immediately adjacent terminating-PSPs but requiring a PSP to have a relationship with all other PSPs so that it can direct caller information to the correct terminating-PSP is a daunting and unnecessary task. The role of the Aggregating Service Provider (ASP) is to provide this routing capability and some high-level ideas are described in Annex A.

The ASP operates as a centralized or regional entity and can determine, based on information included in the PEMEA data object, the best terminating-PSP to direct the information to. There may be more than one ASP across Europe and where this occurs meshing is expected to occur. How the meshing occurs is an operational consideration outside the scope of the present document but may be addressed by subsequent operational considerations.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/54a08e70-27cf-4b6a-5853-5fc33a8b6f7/etsi-ts-103-478-v1.1.1-2018-03

4.3 Interface definitions

4.3.1 Application Interface (Pa)

This is the interface used for communication between the Application and the Application Provider. The exact nature and communication on this interface is out of scope of the present document as this is the interface that allows Application Providers to implement and support service differentiation features in their products. Whilst the implementation of this interface is not in scope of PEMEA, there are specific functions of this interface that a PEMEA-complying implementation shall provide. How these requirements are implemented is out of scope.

4.3.2 Application Provider to PSAP Service Provider Interface (Ps)

This is the interface used by the Application Provider to push caller information to the PSAP Service Provider (PSP). This is a secure interface that requires mutual authentication between the AP and the PSP and a complying AP and PSP shall implement this interface in accordance with the details in the present document when they are not the same entity.

4.3.3 PSAP Service Provider Interface to Aggregating Service Provider Interface (Pr)

This is the interface used by the PSP to route caller information to a different PSP, in which case the sending PSP becomes the origination-PSP (oPSP). The ***Pr*** interface may also be used by the PSP to receive caller information from a different PSP; in this case the receiving PSP becomes the terminating-PSP (tPSP).

This is a secure interface that requires mutual authentication between the oPSP and the tPSP or between the oPSP and the ASP and the tPSP and the ASP. A PSP that wishes to support Application roaming shall implement this interface in accordance with the details in the present document to be PEMEA compliant.

4.3.4 PSAP Service Provider to PSAP Interface (Pp)

This interface is shown for completeness but is outside the scope of the present document. The PSP may provide a simple web interface to the PSAPs it serves or it may integrate the data flows into existing PSAP CPE systems. How this is performed will vary from PSAP to PSAP and from PSP to PSP.

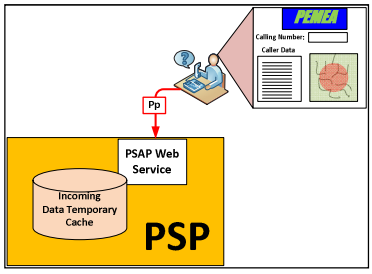

Figure 2: Basic PEMEA PSAP Integration

ETSI STANDARD PREVIEW
(cfastandards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/548b8b2c-327d-4b6a-0853-3333a9b67/etsi-ts-103-478-v1.1.1-2018-03

5 PEMEA functional entity requirements

5.1 Introduction

PEMEA needs to be a secure network and it relies heavily on trust relationships between PSAPs and the entities that they allow to provide information to them. The architecture shown in Figure 1, shows applications connect to application providers (APs) that have trust relationships with PSAP service providers (PSP) that have very strong trust relationships with PSAP. That is, PSAPs trust the PSPs to provide accurate and trustworthy information.

5.2 Application requirements

AA-1: The Application shall detect when the Application is being used and initiate an emergency call.

AA-2: The Application shall authenticate itself to the AP when it sends caller information.

AA-3: At emergency call time the Application shall send the most accurate location of the device as obtained from the device's location APIs and a device timestamp since delay may be considerable.

AA-4: At emergency call time the Application shall send, if it is able to obtain it, the identity of the current point of attachment to the cellular network. At the time of writing this is the full cell-id (MCC-MNC-Cell). However as WiFi becomes more supported as an access technology for cellular operators then the BSSID of the serving WiFi entity may be used instead.

NOTE 1: It is understood that increasingly mobile operating systems are not providing applications access to this information, nevertheless the application should try to acquire it where possible as it may allow for faster routing in some circumstances.

AA-5: The Application shall, if it is able to obtain it, provide the MSISDN of the device to the AP when data is conveyed at call time.

NOTE 2: It is understood that increasingly mobile operating systems are not providing applications access to the MSISDN or IMSI of the device, nevertheless the application should try to acquire this information where possible.

AA-6: The Application shall provide a mechanism for sending location.