ETSI TS 103 755 V1.1.1 (2022-06)

Emergency Communications (EMTEL);
PEMEA ESInet Shared Services

Reference
DTS/EMTEL-00052

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.

1 Scope

The present document describes interoperability, re-use and enhancement of PEMEA and Emergency Services IP network (ESInet) components to ensure seamless integration of Internet Apps and traditional telecommunications service provider solutions and future emergency services offerings. An understanding of the PEMEA architecture is specified in ETSI TS 103 478 [1] and the Core elements for network independent access to emergency services in ETSI TS 103 479 [2], currently named Next Generation 112 (NG112) architecture.

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".

NOTE: Available at https://www.etsi.org/deliver/etsi_ts/103400_103499/103478/01.02.01_60/ts_103478v010201p.pdf.

[2] ETSI TS 103 479 (V1.1.1): "Emergency Communications (EMTEL); Core elements for network independent access to emergency services".

NOTE: Available at https://www.etsi.org/deliver/etsi_ts/103400_103499/103479/01.01.01_60/ts_103479v010101p.pdf.

[3] IANA language subtag registry.

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

[4] IETF RFC 5222: "LoST: A Location-to-Service Translation Protocol", August 2008.

NOTE: Available at https://datatracker.ietf.org/doc/html/rfc5222.

[5] IETF RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", January 2008.

NOTE: Available at https://datatracker.ietf.org/doc/html/rfc5031.

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 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication", June 2014.

NOTE: Available at https://datatracker.ietf.org/doc/html/rfc7235.

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
ASP	Aggregation Service Provider
BCF	Border Control Function
ECRF	Emergency Call Routing Function
EDR	Emergency Data Received (message)
EDS	Emergency Data Send (message)
ESInet	Emergency Services IP network
ESRP	Emergency Service Routing Proxy
ETSI	European Telecommunications Standards Institute
HTTP	Hyper-Text Transfer Protocol
IETF	Internet Engineering Task Force
IM	Instant Messenger
LoST	Location to Service Translation
OTT	Over-The-Top
PEMEA	Pan-European Mobile Emergency Application

PIDF-LO	Presence Information Document Format Location Object
PIM	PSAP Interface Module
PRF	Policy Routing Function
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
RTT	Real-Time Text
SIP	Session Initiation Protocol
SIPS	SIP Secure
SPIF	SIP PEMEA Interworking Function
URI	Uniform Resource Identifier
URN	Uniform Resource Name
XML	eXtensible Markup Language

4 Integrated network view

4.1 Introduction

The ESInet and PEMEA architecture have nodes that perform similar functions but in quite different ways. Consequently there is a need for some of the functions to sit side by side, while some of the more common functionalities can be shared.

4.2 PEMEA ESInet interworking beyond the SPIF

ETSI TS 103 478 [1] defines a basic interworking between PEMEA and SIP via an entity called the SIP PEMEA Interworking Function (SPIF). In this approach, in the absence of a global forest guide network or local public ECRF, an OTT terminal can acquire the SIP address of the local ESInet BCF using the PEMEA network. This approach requires "terminating" the PEMEA signalling at the edge of the emergency network in the SPIF, which consists of a PIM coupled with a SIP-proxy. Such a system allows for basic PEMEA capabilities such as user information and updated location to be provided to Public Safety Answering Points (PSAPs) inside the ESInet, however, it does not allow advanced PEMEA services to be propagated to, and used by PSAPs as there is no way to signal these capabilities to the PSAP.

The present document does not explore the SPIF further, but rather moves the decision point inside the ESInet to the PIM associated with the terminating PSAP. There are a number of advantages to this approach including supporting advanced PEMEA services as well as situations where some services will be delivered via SIP and others via PEMEA giving the PSAP the flexibility to choose.

4.3 PEMEA ESInet interworking architecture

The architecture for PEMEA and ESInet node sharing is shown in Figure 1.

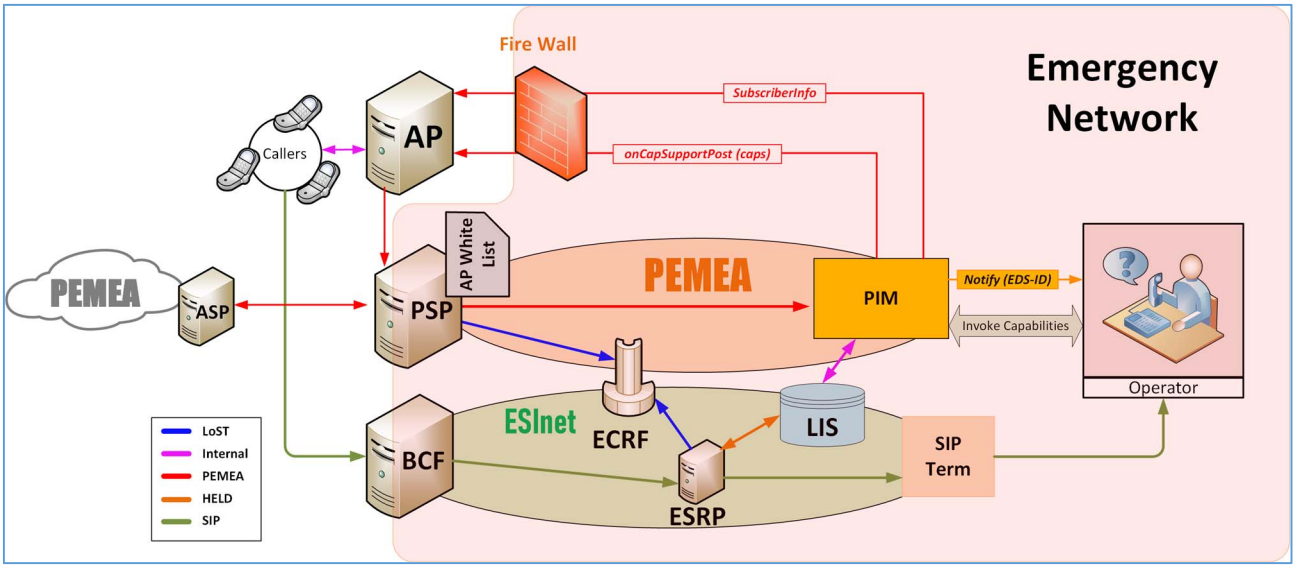

Figure 1: PEMEA and ESInet shared services network architecture

The main operations and interfaces are described in more detail in subsequent clauses of the present document. The PSP acts as the gatekeeping into the shared services network. As described in ETSI TS 103 478 [1], a PSP has a specific relationship with AP that are directly connected to it and these will, in most circumstance, be permitted to communicate with the local PSAP. Whilst PEMEA has been designed to allow applications to roam anywhere in Europe, certain PSAP regions may wish to restrict their access to only certain application providers. The PSP implements this functionality through a permissive white list. This ensures that only valid PEMEA entities that are also on this white list are permitted to enter the shared services network.

5 PEMEA ECRF definitions and procedures

5.1 Overview

The Emergency Call Routing Function (ECRF) uses the Location Service Translation (LoST) protocol as defined in IETF RFC 5222 [4] to transform a location and service identifier into a series of destination identifiers, usually Universal Resource Identifiers (URIs). Different URI types are used for different protocol types, for example SIP or SIPS would be used for the delivery of SIP-based communication services. Similarly, HTTPS URIs destination can be used for the delivery of PEMEA communication messages, and this can be handled natively by the LoST protocol with no required changes to the IETF RFC 5222 LoST protocol specification [4].

5.2 PEMEA service identifiers

5.2.1 Overview

PEMEA was conceived with a single, central service identifier in mind, as a consequence, natively per ETSI TS 103 478 [1], it does not have a concept of sub-services, such as police, fire and ambulance which are easily defined by the service urns used within the ESInet signalling. Despite the promotion of the common 112 number for emergency services in Europe, many member states operate independent numbers for different services and this is a capability that needs to be folded into PEMEA. The support for these services is defined in the subsequent clauses. The guidelines in PEMEA regarding non-understood extensions applies and any implementation that does not understand the service tags extension shall ignore them but pass them through in any EDS routing.

5.2.2 Definition

PEMEA has a philosophy of defining generic containers into which specific capabilities and definitions are bound. Service tag definitions will follow this same approach. The serviceTags element will consist of one or more serviceTags, where each serviceTag consists of a name attribute and a value.

Table 1

Attribute	Meaning
name	This is the identifier of the specific service type. For example: name="serviceUrn". In this case it is saying that the value associated with the service name is to be interpreted as a service urn.
value	Is of type token or of type URI. Complex values are not supported in serviceTags. URIs to retrieve complex values from an external source are a matter for further study.

Specifying a new service requires defining the value type and specifying a new unique name.

EXAMPLE:

```
<serviceTags xmlns="urn:pemea:apps:xml:ns:pemea:servicetags">
   <service name="serviceUrn">urn:service:sos:police</service>
   <service name="forwardLanguage">en</service>
   <service name="forwardMedia">audio</service>
   <service name="reverseLangage">fr</service>
   <service name="reverseMedia">text</service>
</serviceTags>
```

The present document specifies five service options, though not all are relevant to the ECRF routing, the others may be used for policy routing and direction further in the processing pipeline.

Table 2

Name	Value type	Description
serviceUrn	URI	This is the service URN aligning with the service that the user of the application selected. This is the service URN that will be included in any location-based route determination, whether internal to the PSP or ECRF. Service resolution from sub service to top-level service is applied as specified in IETF RFC 5031 [5].
forwardLanguage	Token	This specifies the language that the caller wishes to convey information to the call-taker with. It is a single valid language from [3].
forwardMedia	Token	This specifies the media type that the caller wishes to convey information to the call-taker with. Only one value may be specified. The present document defines the following values: • Text • Audio • Video • Audio_Video
reverseLanguage	Token	This specifies the caller's preferred language to receive information from the call-taker. It is a single valid language from [3].
reverseMedia	Token	This specifies the media type the caller wishes the call-taker to use when conveying information. Only one value may be specified. The present document defines the following values: • Text • Audio • Video • Audio_Video

Use of serviceTags and services is option, and each service shall be have meaning without being dependent on another service being present. Each service should only appear once in the serviceTag list, duplicated service names shall be ignored.

The serviceTags element is sent in the EDS and shall be placed after the accessData element (if one exists) and should be placed before the PIDF-LO.

5.2.3 Service tags schema

The EDS is specified as XML and to maintain compatibility the serviceTags element and services are also specified as XML.

```
<xs:schema
     targetNamespace="urn:pemea:apps:xml:ns:pemea:servicetags"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns:pemeast="urn:pemea:apps:xml:ns:pemea:servicetags"
     xmlns:xml="http://www.w3.org/XML/1998/namespace"
     elementFormDefault="qualified" attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:documentation>
        The present document defines PEMEA service tags.
    </xs:documentation>
  </xs:annotation>

  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
             schemaLocation="http://www.w3.org/2001/xml.xsd"/>

  <!-- define the basic value type URI or token -->
  <xs:simpleType name="valueType">
    <xs:union>
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:enumeration value="any"/>
        </xs:restriction>
      </xs:simpleType>
      <xs:simpleType>
        <xs:restriction base="xs:anyURI">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:union>
  </xs:simpleType>

  <!-- serviceType -->
  <xs:complexType name="serviceType">
    <xs:simpleContent>
      <xs:extension base="pemeast:valueType">
        <xs:attribute name="name" type="xs:token" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <!-- serviceTagType -->
  <xs:complexType name="serviceTagType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:sequence>
         <xs:element name="service" type="pemeast:serviceType" minOccurs="1" maxOccurs="unbounded"/>
        </xs:sequence>xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <!-- ServiceTags element -->
  <xs:element name="serviceTags" type="pemeast:serviceTagType"/>
</xs:schema>
```

5.3 PSP to ECRF query response procedures

A PSP receiving an EDS shall determine where to send it. If the PSP is associated with a PSAP inside an ESInet, then the PSP shall:

1) On receipt of an EDS the PSP shall examine the EDS for a serviceTags element to determine which service URN to use:

   a) If a serviceTags element is not found then the PSP shall use a service URN of urn:service:sos.

   b) If a serviceTags element is present, but does not contain a service of type serviceUrn then the PSP shall use a service URN of urn:service:sos.

c) If a service of type serviceUrn is present but is invalid then the PSP shall use a service URN of urn:service:sos.

d) If a service of type serviceUrn is present and is valid then this value shall be used as the service URN.

2) Construct a findService request using the location provided in the EDS and the service URN select in step 1.

3) Send the findService request to the configured ECRF authenticating either with using a its PEMEA domain certificate or a pre-arranged token such as described in [i.1].

4) The ECRF shall perform its normal procedures as described in ETSI TS 103 479 [2] and IETF RFC 5222 [4]:

a) The ECRF shall be provisioned with HTTPS URI destinations if it is to provide routing information for PEMEA nodes.

b) The HTTPS URIs shall be associated valid PEMEA entities.

c) Each HTTPS URIs shall be associated with either PSP, PIM or ASP.

5) For the proffered location and service urn in the findService request message, the ECRF shall return all valid destination URIs in the mapping element of the findServiceResponse message.

6) The ECRF shall be provisioned with a default mapping. The default mapping for HTTPS responses shall be the default ASP for the PSP. This ensures that the correct PEMEA roaming occurs rather than serving the EDS to a PSAP not associated with the location of the user.

7) On receiving the findServiceResponse from the ECRF the PSP shall determine if the defaultMappingReturned warning is included in the response and if present:

a) The PSP shall inspect the mapping for an HTTPS response URI. If not found then the PSP shall select a configured ASP of last resort. If the address of this ASP is already present in the route element of the EDS then the PSP shall return a PEMEA error message to the node that sent it the EDS with a reasonToken of "circularRoute".

b) If the ASP of last resort is not present in the EDS route element, then it shall verify that the ASP address is in the valid PEMEA entity list. If present it shall add the ASP address to the route element and construct an EDR message. It shall return the EDR to the node from which it received the EDS. The PSP shall then send the EDS to the ASP of last resort.

c) If ASP of last resort is not found in the valid PEMEA entity list, then the PSP shall return a PEMEA error message to the entity from which it received the EDS with a reasonToken of "noRoute".

d) If an HTTPS response is found in the returned mapping then the URI is compared against the valid PEMEA entity list. If the URI is not found in the list then the ASP of last resort is selected and steps 7a through 7c apply.

e) If the URI returned in the mapping is found in the valid PEMEA entity list then PSP verifies that the address is not already present in the EDS route element. If the address is already present then the PSP returns a PEMEA error message to the node from which it received the EDS with a reasonToken of "circularRoute".

f) If the URI is not already present in the route element then it is added to the route element and construct an EDR message. The EDR message shall be returned to the node from which the PSP received the EDS. The updated EDS shall be sent to the identified PEMEA node contained in the mapping.

8) If no defaultMappingReturned warning is present in the returned mapping from the ECRF then:

a) The PSP shall inspect the mapping for an HTTPS response URI. If not found then the PSP shall select a configured ASP of last resort. If the address of this ASP is already present in the route element of the EDS then the PSP shall return a PEMEA error message to the node that sent it the EDS with a reasonToken of "circularRoute".

b) If the ASP of last resort is not present in the EDS route element, then it shall verify that the ASP address is in the valid PEMEA entity list. If present it shall add the ASP address to the route element and construct an EDR message. It shall return the EDR to the node from which it received the EDS. The PSP shall then send the EDS to the APS of last resort.

c) If ASP of last resort is not found in the valid PEMEA entity list, then the PSP shall return a PEMEA error message to the entity from which it received the EDS with a reasonToken of "noRoute".

d) If an HTTPS response is found in the returned mapping then the URI is compared against the valid PEMEA entity list. If the URI is not found in the list then the ASP of last resort is selected and steps 8a through 8c apply.

e) If the URI returned in the mapping is found in the valid PEMEA entity list then PSP verifies that the address is not already present in the EDS route element. If the address is already present then the PSP return a PEMEA error message to the node from which it received the EDS with a reasonToken of "circularRoute".

f) If the URI is not already present in the route element then it is added to the route element and construct an EDR message. The EDR message shall be returned to the node from which the PSP received the EDS. The updated EDS shall be sent to the identified PEMEA node contained in the mapping.

6 Policy routing function integration with PEMEA

6.1 Overview

Policy routing specified in ETSI TS 103 479 [2] is tied heavily to internal ESRP processing and no external interface for querying a PRF is defined. Consequently, there are three clear options available to PEMEA:

1) Define an explicit REST interface for a TerminationPolicy, where the response is a next hop.

2) Periodically acquire the contents of the policy store from each of the destination PSAPs.

3) Perform final destination determination at the PIM that was selected based on location. This may result in the forwarding of the EDS to a neighbour PIM or the processing of the call at the initial PIM.

Options 1 and 2 will be considered for further study should the need arise due to increasing application call rates.

Option 3 shall be the approach taken in the present document.

6.2 Procedures

The PSP at the edge or in the core emergency network will:

1) Extract the service tag from the EDS if there is one, or use the default urn:service:sos if a service tag is not present.

2) Extract the location from the EDS.

3) Query the ECRF with the identified service urn and location using the LoST protocol:

   - Authentication may be based on a pre-arranged token, or asserted identify via a x.509 certificate.

4) Extract the HTTPS response from the return destination URI set:

   - If no HTTPS URI is included in the response set, then a default URI is configured in the PSP.

5) Direct the EDS to the destination URI:

   - This will either be a PIM (usually the case).

   - Or it may be a downstream PSP, in which case the PSP procedures are repeated by this destination.

At the initial PIM:

1) General policy relating to things such as:

   a) Capabilities proffered

b) Included service tags

c) Time of day

d) PIM call occupancy

Are considered and, depending on the outcome of the consideration the EDS maybe:

e) Responded to immediately by sending an onCapSupportPost and binding the PEMEA session to the answering PIM.

f) Held and forwarded to 1 or more neighbouring PIMs. This is usually the case if waiting for a legacy voice call to be aligned with the PEMEA data. This case is covered more in clause 7.4.

g) Forwarded to a single more appropriate PIM based on current PIM status.

2) The final PIM, depending on proffered and overlapping capabilities may respond to the AP by sending an onCapSupportPost message with the common subset of capabilities and thus binding the PEMEA session between the AP and the PIM.

7 EDS forwarding

7.1 Overview

EDS forwarding between PIMs in the context of policy routing is allowed. Whilst there may be any number of reasons for forwarding an EDS the present document identifies the following:

1) A parallel voice call is anticipated to align with the PEMEA data.

2) The PSAP is congested or otherwise unavailable.

3) Requested services not available at the initial PSAP.

The rules that apply to these various forwarding conditions are described in detail in the clauses that follow.

7.2 PEMEA Error message reasonTokens

ETSI TS 103 478 [1] defines the error reason tokens in table 12, this table is enhanced in the present document to include responses for resourceContention and serviceUnavailable. The complete list of reasonToken is provided in Table 3.

Table 3: Error reasonToken values

Value	Description
ttlExhausted	The time to live value reached zero and the message was not delivered to a PSAP.
noRoute	The entity currently responsible for routing the message does not have a relationship with any entity that can receive it.
badMessage	The message could not be understood by the receiving entity (normally this message will be sent by the home PSP).
circularRoute	The entity currently trying to route the message has identified that the next hop it would send the message to is already in the route element.
duplicateHopPosition	The route element contained two or more hops with the same position attribute value.
httpError	The entity trying to send the EDS message encountered an HTTP error from the next hop. The error type should be contained in the message element.
resourceContention	This error is generally returned by a PIM that has insufficient resources available to be able to process the call.
serviceUnavailable	This error may be sent in response to an EDS where none of the auto-response capabilities are available at the PIM.

7.3 Common forwarding rules

The following forwarding rules apply to each of the forwarding reasons identified in clause 7.1:

1) A PIM may have a set of neighbour PIMs to which it may forward EDS messages.

2) A PIM may have a set of neighbour PIMs from which it may receive EDS messages. This may be the same set as 1.

3) A PIM shall never forward an EDS if it has replied to the AP with either and onErrorPost or an onCapSupportPost.

4) A PIM shall never forward an EDS that it has received from another PIM.

5) A PIM shall never respond to an EDS from a PIM with an EDR if the EDS contains auto-response capabilities unless it can handle the associated session.

6) A PIM shall respond to an EDS from a PIM with an EDR if the EDS does not contain any auto-response capabilities.

7) A PIM shall only forward an EDS containing capabilities requiring auto-responses to one PIM at a time and shall stop forwarding on receipt of an EDR.

8) A PIM may try to forward the EDS to a subsequent PIM should it receive an error from the currently tried PIM.

9) If the PIM is unable to successful forward the EDS to a neighbour PIM, it should provide what service it can. It shall respond to the AP with an onErrorPost in the event it cannot support the request in any capacity.

7.4 Parallel voice call

PEMEA supports capabilities that require an immediate answering by the PIM, in such cases the PIM, if it supports the requested capability, sends an onCapSupportPost message with the supported capabilities to the originating AP. An example of this kind of capability is the SIP_Request capability. However, some PEMEA EDS messages include only capabilities that provide ancillary data to a voice call, things such as location updates or user information, for example.

In the case where a PIM receives an EDS that does not contain any capabilities that require an immediate answer then it shall refrain from sending an onCapSupportPost message until the associated voice call has arrived at the PSAP. The remainder of this clause refers only to the case where there are no auto-response capabilities in the EDS and a voice call associated with the EDS is expected.

If the PIM is configured with a neighbour list of PIMs then it shall forward the EDS to ALL PIMs in the list. The originating PIM shall expect to receive an EDR from each PIM unless the PIM/PSAP is not able to handle the call even if a corresponding voice call arrives. In this this case, the PIM that does not send an EDR, shall instead send an error. The PIM receiving the error shall log the response but shall not send an onErrorPost message.

On receipt of the EDS for which an EDR has been sent in reply, each PIM shall start a timer with the expectation that the call will arrive prior to the timer expiring. PIMs that have had the EDR forwarded to them shall silently delete the EDS from their cache once the timer has expired. The PIM that initially received the EDS shall send an onErrorPost to the originating AP should its timer expire.

Each PIM receiving the EDS, including the original PIM shall cache the EDS and wait for a voice call. On receipt of the voice call, the PIM associated with the PSAP that has received the call shall send an onCapSupportPost to the originating AP binding the emergency session between the AP and the answering PIM. At this point, the AP shall ignore any messages from a PIM except for the PIM to which the emergency session is bound (the answering PIM). Should the AP receive an onErrorPost from a PIM after the emergency session is bound, then the onErrorPost message shall be ignored by the AP.

If all PIM sessions timeout prior to a voice call arriving at one of the PSAPs then the PIM that first received the EDS shall send an onErrorPost to the originating AP. If the emergency session at the AP has not been bound to a PIM, then the emergency session in the AP shall report an error to the App and follow the directions for session clear down prescribed in ETSI TS 103 478 [1].

The procedures above address the cases where one or more PSAPs have an unusually high-call rate or is unable to handle a voice call and so the calls are distributed to neighbouring PSAP. They also address the issue where the EDS and the voice call have not arrived at the same PSAP due to difference in routing owing to differences in accuracy of the location information provided at the time the messages were sent.

7.5 PSAP unavailable

There are circumstances where a PSAP destination returned by the ECRF is simply unavailable. That is, when the PSP tries to contact the PIM and it gets an HTTP 5XX error or a PEMEA error message indicating congestion or resource contention. In such a circumstance the PSP may be configured with a fallback PIM. The fallback mechanism may be:

- A single fallback PIM for PSP.
- An ordered list of PIMs to try.
- An ordered list of PIMs to try where the list is associated with the PIM address returned by the ECRF.

If the PSP receives an error from the PIM whose address was returned by the ECRF, and the PSP is not configured with a fallback PIM address then the PSP shall send an onErrorPost to the originating AP.

If the PSP receives an error from the PIM whose address was returned by the ECRF, and the PSP is configured with one or more fallback PIM addresses then the PSP shall:

1) Select the highest priority PIM and send the EDS to this PIM.
2) If the PSP receives an EDR from the PIM then the PSP stops further processing of that emergency session.
3) If the PSP receives a 5XX or a PEMEA error message in response to the EDS then PSP shall selected the highest priority PIM and repeat step 2.
4) If the PSP has exhausted all configured PIMs without receiving an EDR then the PSP shall send an onErrorPost message to the originating AP.
5) If the last error message received as an HTTP Error code, then the error reason in the onErrorPost message shall be set to httpError.
6) If the message received from the last PIM was a PEMEA error message then this shall be sent in the onErrorPost message.

7.6 Requested services unavailable

Sometimes, a call gets directed to a PSAP that does not have the preferred communication service available. Clause 5.2 defines service tags for PEMEA that allow the caller to specify their preferred communication media and languages. A PIM may have a list of neighbour PIMs and may identify communication capabilities with these. In a case where the communication preferences in the service tags are not available at a PIM receiving an EDS from a PSP, that PIM may forward the EDS to a neighbour PIM, if the neighbour PIM is known to support the requested communication mechanism.

Service tags are an optional element in the EDS and if they are not provided then the requested services are solely contained in the apMoreInformation extension elements. If communications services, such as IM, Audio_Video or RTT are included in the capability set, and one of these services is supported by the PIM, then PM shall send an onCapSupportPost to the AP. If none of the services are supported by the PIM, but the PIM has a neighbour PIM that can support one or more of these services, then the PIM may forward the EDS to that PIM.

If a PIM receives an EDS from a neighbouring PIM and it is unable to support any of the communication preferences in included in the service tags component or any of the capabilities included in the apMoreInformation element, then the PIM shall respond to the EDS with an error with the reason token of serviceUnavailable. A PIM receiving an error message with a reason token of serviceUnavailable shall relay the error to the AP using the onErrorPost procedure from ETSI TS 103 478 [1].

Annex A (informative): Bibliography

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

NOTE: Available at https://datatracker.ietf.org/doc/html/rfc6753.

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

NOTE: Available at https://tools.ietf.org/html/rfc4119.

History

Document history		
V1.1.1	June 2022	Publication