PEMEA CONSORTIUM

Connecting internet apps to emergency services

PEMEA Operations Document

PEMEA-CONS-OPS-001

V10.3

June 2023

Contributors

Name	Company
Luca Bergonzi	Beta80
Bertrand Casse James Winterbottom Javier Cabas Jorge Forcada	Chapsvision / Deveryware
Evangelos Markakis	PEMEA Consortium Chairman/ HMU
Urban Sedler	University of Ljubljana

Table of Contents

1. Objectives of the document

This document describes the operational model of the PEMEA network. It describes the different concepts PEMEA operatives and how they fit into the overall PEMEA ecosystem.

It aims to explain how PSAPs can interconnect with the PEMEA network to receive emergency communications made from Internet applications.

It aims to explain how creators of Internet applications can interface their applications to the PEMEA network and enable emergency calling for their users.

This document does not explain how organizations that wish to develop PEMEA network nodes, AP, PSP, ASP, PIM, can bring their nodes into the PEMEA network. A formal procedure for this shall be produced in the future, in the meantime, organizations wishing to develop and link PEMEA nodes into the PEMEA network should contact the PEMEA Consortium for details.

2. Terms and Definitions

2.1 Abbreviations

The following terms and definitions are used in this document:

App	Application
AP	Application Provider
CAD	Computer Aided Dispatch
EDS	Emergency Data Send
EMTEL	Emergency Communications
ESInet	Emergency Services Internet
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
GDPR	General Data Protection Regulation
PEMEA	Pan-European Mobile Emergency Application
PIM	PSAP Interface Module
PRA	PEMEA Registration Authority
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
PSTN	Public Switch Telephone Network
RTT	Real-Time Text
TS	Technical Specification

2.2 Definitions

The understanding of the following definitions is required to fully appreciate the concepts described in this document.

Application	Software providing communication capabilities that can support emergency calling. This may be a dedicated emergency calling application, or it may be a more general application to which emergency calling functionality is added.
Application Creator	The organization or entity that write the application that is able to initiate emergency calls.
CAD	Refers to internal PSAP systems responsible for handling incoming calls, transfering them to call-takers and to first responder agencies.
Call-taker	A person working within a PSAP responsible for answering emergency calls.
PEMEA Consortium	The organization responsible for ensuring the interoperability, integrity, quality, security, and growth of the PEMEA network.
PEMEA Network	All active and inter-linked PEMEA Nodes registered with the PRA
PEMEA Nodes	The PEMEA entities defined in TS 103 478 [1] comprised of the AP, PSP, ASP, PSAP/PIM.
PEMEA Operator	A PEMEA operator is an entity that manages the deployment and day to day administrative and operational functions of a PEMEA node in the PEMEA network. A PEMEA operator may operate a single node, such as an AP or, a complete network segment such as an AP, PSP, ASP and PIM.
PEMEA PSAP User	A PSAP or emergency agency that makes use of PEMEA services to PEMEA enable their PSAP. In this document it refers to a PSAP that has integrated their CAD system to a PSAP Interface module run by a PEMEA Operator.
PEMEA testing partner	An organization or entity recognized by the PEMEA Consortium as being able to provide conformance testing capabilities for organizations wishing to become registered PEMEA vendors.
PEMEA AP Users	Application Creatorsthat make use of PEMEA Operator AP Nodes to connect to their Apps to the PEMEA network for making emergency calls.
PEMEA Vendor	A PEMEA vendor is an entity authorized to provide PEMEA nodes that are certified to comply with the technical and procedural PEMEA standards for a specific node-type.
PIM	The PSAP Interface Module is a module that is tightly integrated with

	the PSAP CAD system making the PSAP a direct PEMEA node.
PSAP	Public entity offering an answering point for emergency calls initiated by members of the public.
Public	The users of applications for the purpose of making emergency calls. These may be citizens or visitors to the country where the emergency call is placed and ultimately terminated.

3. What is PEMEA?

Today, more people communicate using Apps more than any other means. There are hundreds of Apps whose primary function is communications, available globally for all manner of devices, from smartphone to tablets, laptops, desktops and browser. This number expands even more when we consider Apps whose primary purpose is something other than communications but include some type of communications channel to enhance their primary function, for example a chat or messenger capability added to a shopping App.

Dedicated emergency applications have also been produced by regions and countries to provide enhanced location and advanced multi-media services to improve emergency communications overall, and in particular for people with hearing and speech difficulties.

Many enterprises now use integrated multi-media applications as their primary means of communication. These solutions use cloud-based servers and provide global access as well as inter-enterprise domain calling, resulting in little to no need for traditional PSTN calling access.

Whilst all these Apps may be different, they all use web-based technologies focussed around WebRTC and HTML-5 and associated security technologies. The Pan-European Mobile Emergency Application framework (PEMEA) was developed to enable applications to connect to the most appropriate PSAP no matter where the user is, in a common and standard way, whilst ensuring security, privacy, authentication, authorization and integrity of the PEMEA network and the nodes from which it is comprised.

The core PEMEA specification [R.1] doesn't define multi-media communications between the caller's App and PSAP, but rather provides a enabler for such communications to be intiated in a secure peer-to-peer fashion. The multi-media communications themselves are defined in separate specifcations that include information about how the capability is invoked and managed within the scope of the PEMEA framework. This makes PEMEA extremely powerful in terms of network evolution, as it allows some networks and Apps to move faster than others without underming the integrity of the network. Examples of PEMEA multi-media extensions include Instant Messenge (Chat) TS 103 756 [R.2] and Real-Time Text (RTT) TS 103 871 [R.3].

4. Connecting to the PEMEA network

4.1 Overview of the PEMEA ecosystem

The PEMEA protocol is deliberately simple to ensure minimal issues with interoperability. One of the key reasons for this is that PEMEA is intended to be near universal, meaning that direct interoperability testing between every single deployed system and every new or updated system is not practical or in many cases even possible. So a different approach to that employed by more traditional network operators is required.

The PEMEA Consortium, which currently manages the "PEMEA Network", only allows nodes to be connected to the PEMEA network if they are sourced from an acredited PEMEA vendor. PEMEA vendor equipment is certified by authorized PEMEA testing partners for compatibility and interoperability with other PEMEA vendor equipment.

Application creators build their Apps or App servers to use a PEMEA AP Vendor's Pa API. In this way the PEMEA AP vendor is able to certify that the App complies with their Pa API, and since the PEMEA AP Vendor's AP is already PEMEA certified, by association, the App creator's App becomes a certified PEMEA App.

Similarly, creators of PSAP CAD equipment integrate to use the PEMEA PIM Vendor's API. In this way the PEMEA PIM vendor is able to cetify that the PSAP CAD complies with their API and since the PEMEA PIM Vendor's PIM is already PEMEA certified, by association, the CAD becomes certified as being PEMEA compliant.

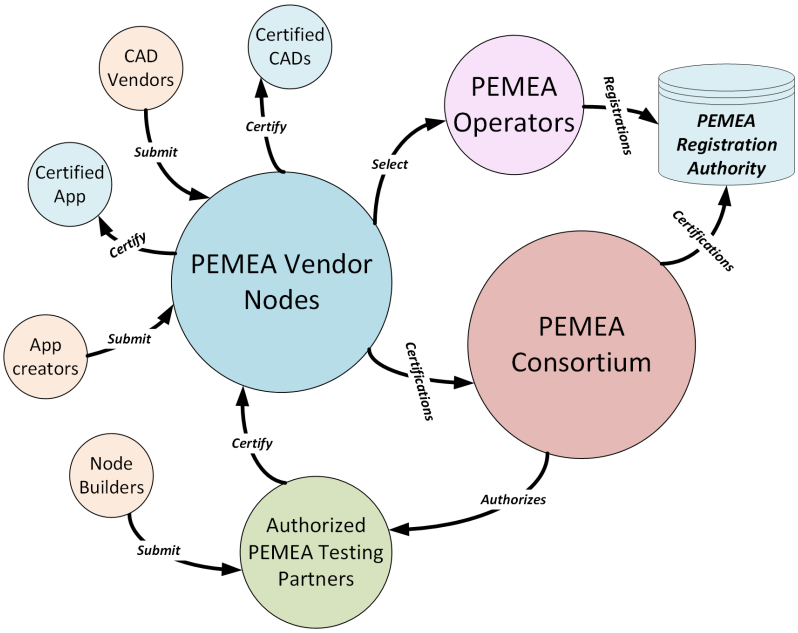

Figure 1: PEMEA Ecosystem

Figure 1 illustrates the previously stated delegated certification approach taken by PEMEA to ensure that all entities in the network can interoperate correctly.

The PEMEA Consortium authorizes PEMEA testing partners
Node builder submit their nodes for certification by the PEMEA testing partners
Nodes that pass the necessary tests are certified as being PEMEA compliant.
The PEMEA Vendor can submit their certifications to the PEMEA Consortium
App creators can submit their Apps for validation by PEMEA AP vendors.
Apps that pass the necessary tests are certified as being PEMEA complient to a particular vendor's AP.
The PEMEA Vendors submit App certifications to the PEMEA Consortium.
CAD vendors can work woth PEMEA PIM vendors to integrate their solutions
CADs that intgerate sucessfully with a PEMEA PIM vendor become PEMEA complient to that vendor's PIM.
The PEMEA vendors submit the CAD certifications to the PEMEA Consortium.
The PEMEA Consortium passes all certifications to the PEMEA Registration Authority.
PEMEA Operators select PEMEA nodes from PEMEA vendors for use in the PEMEA network.
PEMEA Operators register the specific operational PEMEA nodes with the PEMEA Registration Authority.

Authorization and authentication of valid PEMEA nodes is performed with the assistance of a special node called the PEMEA Registration Authority (PRA). A valid PEMEA node is one that has been created by a PEMEA vendor and is correctly configured and registered with the PRA. The PRA then makes available a list of all valid PEMEA entities. This list is downloaded, at least every 24 hours, by each PEMEA node. Connectivity between PEMEA nodes and the data made available is subject to entities being in this list and to the node type access rules described in TS 103 478 [R.1].

Figure 2 shows how the PEMEA nodes interconnect and interact with the PRA to ensure the integrity of the PEMEA network.

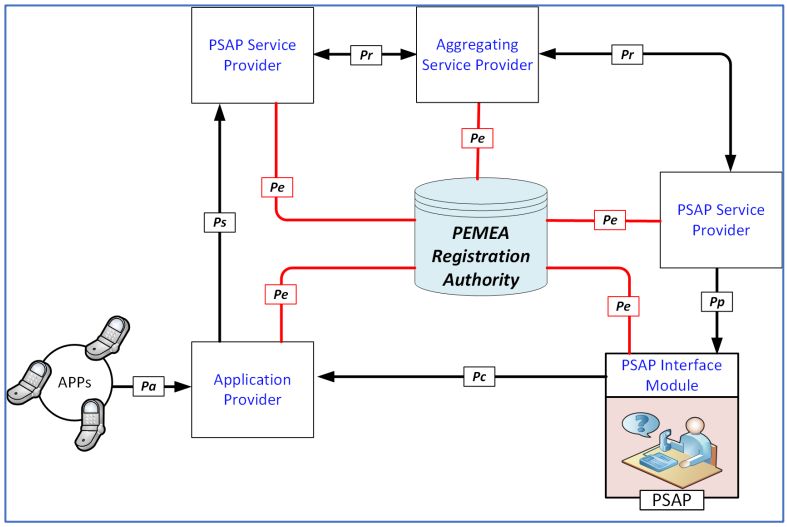

Figure 2: PEMEA Nodes and the PRA

4.2 Application creators

4.2.1 Description

These are the entities/organizations that create and/or operate an Internet communications App. These Apps need to connect to the PEMEA network through an AP that is supplied by a PEMEA AP Vendor. App creators may inlcude small dedicated local emergency applications, large publically available communications Apps, or global cloud-deployed enterprise communications solutions.

By choosing a PEMEA AP Vendor, the App creator need only integrate against that AP vendor's API in order to gain certification to operator in the PEMEA network. This is the fastest and most cost effective way for an App creator to deploy their App into the PEMEA network.

Depending on the PEMEA AP Vendor chosen, they may have more than one way to connect an App. In some cases the App creator has an application server that performs all necessary user authentication and authorization procedures, and it brokers any emergency request to the AP. From the AP standpoint, it only needs to authenticate and authorization the application server on a per emergency communication session basis. Other connection models might allow Apps to connect directly to the AP. In such a case the App authernication and authorization obligations pass to the AP. These connection options are shown in Figure 3.

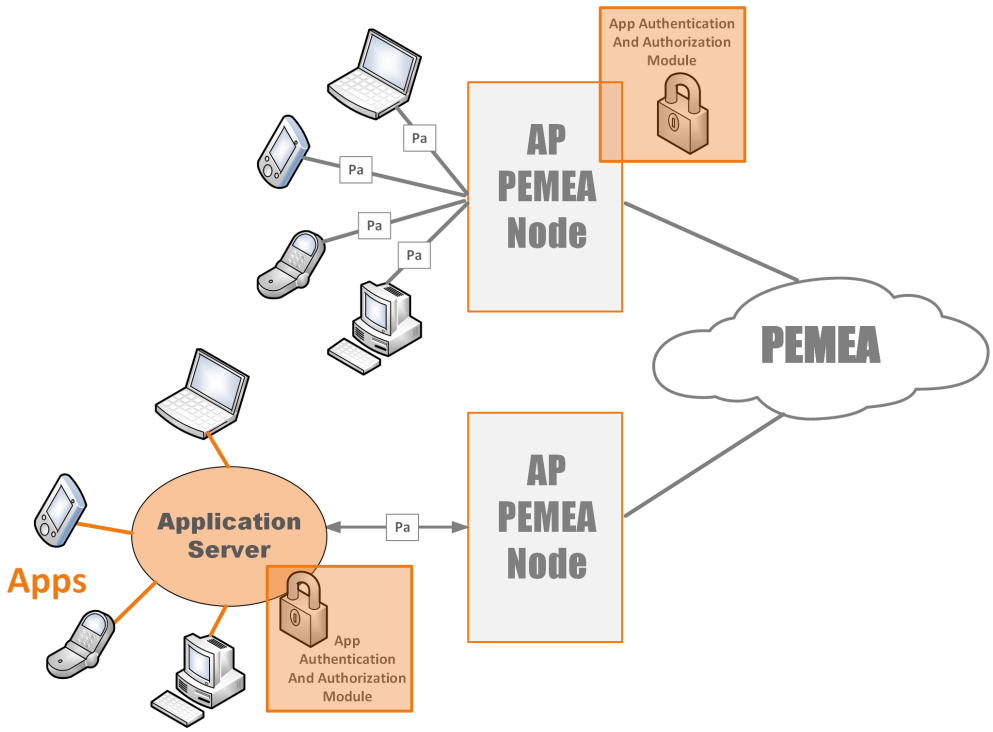

Figure 3: AP connection options

New capabilities are being introduced to PEMEA by a range of different organization, including ETSI, the PEMEA Consortium, as well as private and public organizations. The PEMEA Consortium, through the PRA, maintains a list of generally recognized capabilities, and the certified functionality for each AP is included in the valid entities files provided by the PRA.

Not all PEMEA AP Vendors offer all capabilities, and not all Apps may choose to implement all capabilities offerred by an AP. It is the responsibility of the PEMEA AP Vendor to validate that an App complies with all of its APIs necessary for providing the desired capabilities and functionality.

4.2.2 Application certification

Prior to the App being able to connect to the PEMEA network, the PEMEA AP Vendor must certify that the application is suitable for use in emergency calls. This involves validating functionality, reliability and resilience. Ensuring that 24/7 support procedures and arrangements exist to ensure fast issue resolution and return to service. All of these aspects must be addressed prior to the PEMEA AP Vendor certifying the application suitable for connectivity to the PEMEA network and registering this certification with the PEMEA Consortium.

Once the App is certified, the certification is published the PEMEA Consortium webpage.

4.2.3 Application certification renewal

The certification should be renewed annually to ensure that interfaces between the Application and the PEMEA AP Vendor continue to operate as expected. Recertification is also required if the App or PEMEA AP Vendor is to add new functionality to support PEMEA capabilities. The certified support for the new capabilities is registered with the PEMEA Consortium and PRA so that it will be included in the PRA PEMEA entities file.

4.3 Third-party emergency providers

4.3.1 Description

A third-party emergency provider is generally a private organization that “brokers” communications between the person/system/organization in need and the most appropriate emergency centre to handle that situation, based on location and the type of situation. In some ways, these can be thought of specialized Apps.

Often, the initial communication is to a national or centralized European call-centre, and from there a communication is initiated into the PEMEA network to find the correct PSAP. The communication channels are then linked from the caller equipment to the PSAP via the third-party agency.

Organizations that may provide these kinds of services may be eCall centers, insurance companies, or premium roadside assistance services.

These types of deployments integrate with an existing PEMEA AP Vendor node, with the third-party provider equipment managing user authentication and authorization, and the AP authenticating and authorizing the third-party provider equipment. This is shown in Figure 4.

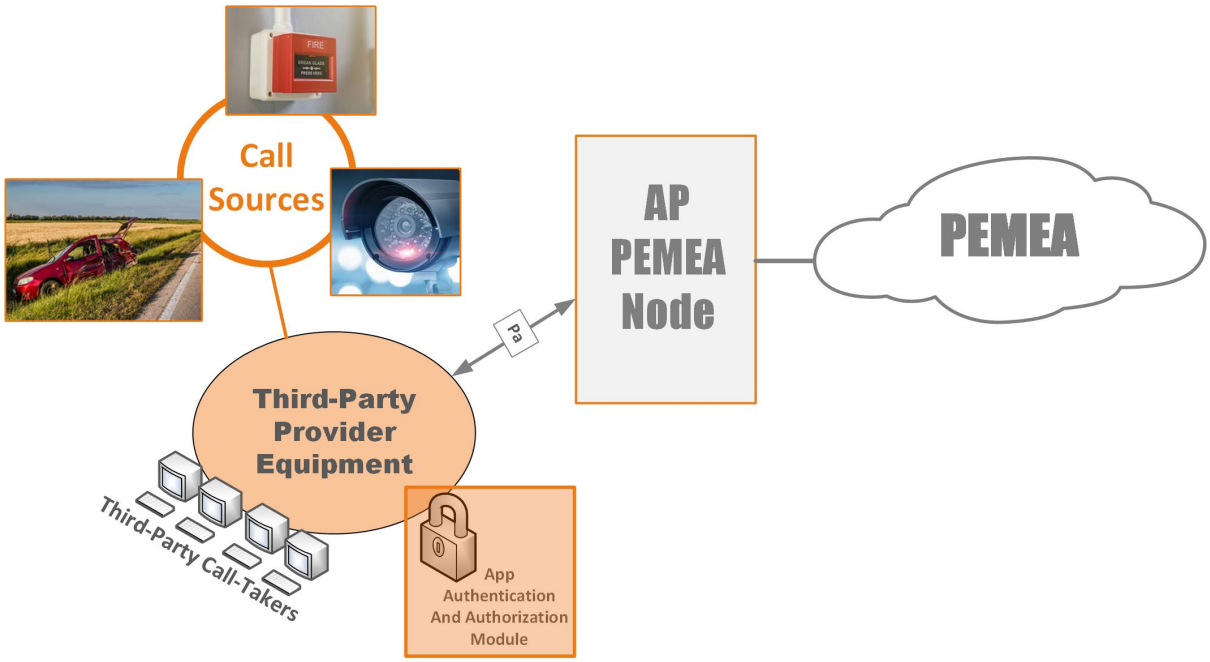

Figure 4: Third-Party provider deployment

New capabilities are being introduced to PEMEA by a range of different organization, including ETSI, the PEMEA Consortium, as well as private and public organizations. The PEMEA Consortium, through the PRA, maintains a list of generally recognized capabilities, and the certified functionality for each AP is included in the valid entities files provided by the PRA.

Not all PEMEA AP Vendors offer all capabilities, and not all third-party providers may choose to implement all capabilities offerred by an AP. It is the responsibility of the PEMEA AP Vendor to validate that a third-party provdier complies with all of its APIs necessary for providing the desired capabilities and functionality.

4.3.2 Third-party provider certification

Prior to the third-party provider being able to connect to the PEMEA network, the PEMEA AP Vendor must certify that the third-party provider is authorized to support emergency calls. This involves validating functionality, reliability and resilience. Ensuring that 24/7 support procedures and arrangements exist to ensure fast issue resolution and return to service. All of these aspects must be addressed prior to the PEMEA AP Vendor certifying the third-party provider is suitable for connectivity to the PEMEA network and registering this certification with the PEMEA Consortium.

Once the third-party provider is certified, the certification is published the PEMEA Consortium webpage.

4.3.3 Third-party provider certification renewal

The certification should be renewed annually to ensure that interfaces between the third-party provider systems and the PEMEA AP Vendor continue to operate as expected. Recertification is also required if the third-party provider systems or PEMEA AP Vendor is to add new functionality to

support PEMEA capabilities. The certified support for the new capabilities is registered with the PEMEA Consortium and PRA so that it will be included in the PRA PEMEA entities file.

4.4 PSAPs and CADs

4.4.1 Description

Public Safety Answer Points, PSAPs, as the name suggests, exist to provide emergency call-taking functions for the general-public. Responsible PSAPs that recognize the significance of the App usage by members of the public and want to CAD equipment that interfaces with the PEMEA network.

The PEMEA PIM Vendors provide easy to implement APIs that can be used by the CAD. The PIM/tPSP perform all of the necessary PEMEA signalling and interactions with the PEMEA network Nodes, including the implementation of simple data retrieval and advanced multi-media service capabilities.

CAD vendors can perform integration tests with PEMEA PIM Vendors for the desired PEMEA capabilities. Once passed, a PEMEA certification is provide to the CAD vendor and sent by the PEMEA PIM vendor to the PEMEA Consortium. Not all PEMEA PIM Vendors or CAD support all possible PEMEA capabilities, so the certification only includes the functionality that was actually tested.

PSAPs should choose the PEMEA PIM Vendor and CAD vendor that best provides the capabilities to suit their needs. The PEMEA Consortium has published a PEMEA Tender Requirements Recommendation document [R.5] to assist PSAPs with understanding what PEMEA capabilities exist and should be included within their tendered systems.

The PIM/ tPSP may be operated by a third-party in a cloud environment or it may be deployed in the same data centre group as the CAD. The PIM/ tPSP needs to offer the same degree of resilience as the CAD solution particularly when it comes to the management of multi-media communications.

Once a PSAP has selected their provider they should perform the necessary integration tests with that provider to ensure that all functionality is operating as expected. Once this is done, the PEMEA node Operator can register the PIM with the PRA so that the PSAP entity is included in the PRA PEMEA entities file.

4.4.2 Deployments

A PSAP or group of PSAPs may wish to control their own PSP and ASP. This is allowed, but each node must be uniquely registered in the PRA and each node must comply with the domain name and certificate requirements as laid out in TS 103 478 [R.1]. This is to ensure that other nodes in the PEMEA network know exactly the type of node that is trying to connect to them so that the correct access policies can be applied. The PRA is constructed in such a way as to reject duplicate domain names for nodes. However, if a common certificate is shared across nodes of different types, then any receiving node will apply the rules associated with the least trusted node type, the ASP, resulting in significant loss of functionality.

It is the role of the PEMEA node Operator to ensure that this rule on domain names is adhered to.

4.4.3 Access controls

PSAPs and other emergency agencies are protective of their networks and at times wish or need to impose tighter access restrictions to their network than are provided by the rigors outlined in this document. In such cases a PSAP is allowed to control which PEMEA nodes and Apps may originate messages to it. This can be done by way of a white-list or black-list in any of the ASP, PSP or PIM nodes.

No notification to the PRA is required should an agency elect not to terminate any requests from a given source.

If an agency moves to block a particular source due to spamming or unusually high traffic-volumes then it is recommended that the agency contact both the PRA and operator of the node so that further analysis as to the cause of the issue can be performed. This allows actions to be taken close to the source of the issue rather than at the terminating node. If the operator of the source node does not take action to resolve the issue, then the PRA reserves the right to deactivate the node in the PRA thereby removing it from the valid entity list.

5. PEMEA Registration Authority (PRA)

5.1 Role

The role of the PRA is vital to the functioning, security and integrity of the PEMEA network, as it provides the trust anchor for all nodes in the network. The PRA can therefore be thought of as the PEMEA network watchdog and it maintains:

- List of all registered PEMEA extensions
- Contact details for any registered entity
- List of currently registered and active PEMEA entities
- When an entity last downloaded an entities file
- Any changes made to PRA and by whom
- PEMEA node Vendors
- PEMEA testing partners

5.2 Types of registration

All entities in the sphere of the PEMEA ecosystem need to be registered, and in order to register some degree of certification is required.

Apps, third-party providers and PSAPs receive their certification from their PEMEA Vendor, and it is the responsibility of the PEMEA Vendor to register the associated AP, PIM or tPSP instance with the PEMEA Consortium as part of the certification process.

PEMEA Vendors and authorized PEMEA testing partners need to be registered with the PEMEA Consortium. The requirements for obtaining the necessary certification to register as a PEMEA vendor or PEMEA testing partner are not addressed in the present document. However, certification for enrolling as one of these entities is done so on a per node-type and per capability basis.

That is, a PEMEA vendor must hold a valid registration for each node type that it is allowed to sell, as well as which capabilities that node is certified to support. This ensures that an AP, for example, can only register an App for capabilities that the AP is certified to provide.
New PEMEA capabilities can also be registered with the PRA. This registration request needs to come via the PEMEA Consortium and more is covered on this in Section 6.3.

5.3 Operation

5.3.1 Overview

The PRA is operated by the PEMEA Consortium and is independent of any PEMEA vendor or Operator. The PEMEA Consortium maintains the list of certified PEMEA Vendors, and PEMEA Operators may only register PEMEA nodes with the PRA that are provided by a certified PEMEA Vendor.

Entities registered into the PRA to be included in the valid entities file must include contact details for the agency/entity that is operating the node. This is so the PEMEA node Operator can be contacted in case of anomalies or complaints from other PEMEA node Operators.

PEMEA nodes are required to periodically download the PEMEA entities file to ensure that all valid PEMEA entities are able to provide service. Failure to download the entities file within a given period will result in the node operator being sent an email indicating the failure. Continued failure to download the list may result in PEMEA node deactivation occurring.

5.3.2 Notifications

The PRA may send notifications to PEMEA node Operators for a variety of reasons including:

- Node deactivation
- New node activation
- Identified network issues.

Notifications may be generated for certain node types, for example a new ASP or PSP coming on line. In this situation, the notification may be sent to existing ASP and PSP PEMEA Operators so that they can update their routing rules.

5.3.3 Contacting the PRA

The PRA is currently operated and managed by the PEMEA Consortium. Initial requests for PRA action should be addressed to **pra@pemea.help.**

6. PEMEA Consortium

6.1 Role

The PEMEA Consortium is a Non-Government Organization (NGO) established to coordinate, manage and ensure the integrity of the PEMEA ecosystem. This includes, presently, the general administration of the PRA.

6.2 Structure

The PEMEA Consortium's membership is comprised of public safety agencies, infrastructure vendors, application creators, academic institutions, special interest groups and individuals interested in expanding and improving the PEMEA ecosystem in delivering best possible solutions for public safety.
Anyone can join through the PEMEA Consortium web page https://pemea.help/be-a-member/.

In addition to its general membership, the PEMEA Consortium has an executive advisory board that sets the direction of the Consortium and its agenda for the next reporting period. In addition to this, the advisory board reviews recommendations put forward by the PEMEA Consortium members for inclusion into the PEMEA ecosystem. Such recommendations may include:

- New PEMEA capabilities
- New operating procedures or documents
- Updates to operating procedure or documents
- Changes to the PEMEA Consortium webpage
- Webinars on specific topics

6.3 Adding new PEMEA capabilities

PEMEA is a service enabler, that is, it has a standard way to define a capability and to deliver that capability offering from an Application to a PSAP. Invocation of that capability is entirely up to the PSAP. This approach allows for very fast introduction and testing of new capabilities to address certain needs without the need to enable the capability across the entire PEMEA network.

Once a capability has been tested and the organizations or entities that have defined it are happy with the outcome, they may request that it be recognized as a general PEMEA capability. The PEMEA Consortium executive advisory board assesses the Capability, with one criterion being a publicly available specification and others around patents and any royalties required for implementers.

6.4 Awareness and information

The PEMEA Consortium has a publicly accessible web site at https://pemea.help. This site contains all information about the PEMEA Consortium, including this document and numerous other sources.

The PEMEA Consortium holds quarterly Webinars and publishes biannual newsletters. The there is also a PEMEA Consortium LinkedIn page where information about new PEMEA activities and deployments are posted.

7. References

7.1 Normative References

[R.1] ETSI TS 103 478: EMTEL; Pan-European Mobile Emergency Application framework
[R.2] ETSI TS 103 756: EMTEL; PEMEA Instant Message Extention
[R.3] ETSI TS 103 871: EMTEL; PEMEA Real-Time Text Extension
[R.4] ETSI TS 103 755: EMTEL; PEMEA ESInet Shared Services
[R.5] PEMEA-CONS-Tender-001: PEMEA Consortium; Guidelines for Including PEMEA in tenders

7.2 Informative References

8. HISTORY

Document history		
V10.0	17 August 2022	Initial Draft
V10.1	7 October 2022	Significant changes to terminology and operator model to avoid confusion and to clearly spell out the different PEMEA actors
V10.2	26 October 2022	Minor updates
V10.3	7 June 2023	Minor corrections