

EENA Operations Document

Pan-European Mobile Emergency App (PEMEA) Approval Procedure Phase I

Title	PEMEA Approval Procedure		
Version	1.0		
Revision date	07-06-2014		
Status of the document	Draft	For comments	Approved



Authors and contributors to this document

This document was written by members of EENA:

Authors	Country / Organisation
Bertrand Casse	Deveryware / Vice-Chair EENA Operations Committee
James Winterbottom	EENA / Vice-Chair EENA Technical Committee

Contributors	Country / Organisation
Iratxe Gomez	ATOS / Co-Chair EENA Operations Committee
Cristina Lumbreras	EENA
Luca Bergonzi	Beta80/ Co-Chair EENA Operations Committee



Legal Disclaimer

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.



Table of contents

1	Executive Summary	5
2	Abbreviations and References	5
2.1	Abbreviations.....	5
2.2	References	5
3	PEMEA Application Approval.....	6
3.1	Process Overview	7
3.2	Role of the PEMEA registry authority	8
3.3	Initial registration process	8
4	PEMEA Implementation process overview	9
4.1	Phase I process.....	9
4.1.1	Implementation requirements overview	9
4.1.2	PEMEA Entities role description	10
4.1.3	End of phase I	10
4.2	Phase II process.....	11
5	Conclusion.....	11
	ANNEX.....	12



1 Executive Summary

The purpose of this document is to provide all entities, application providers, PSAPs service providers, PSAPs and aggregating service providers the necessary operational procedures and guidelines for using the Pan-European Mobile Emergency Application (PEMEA) framework.

As explained in [R3], PEMEA architecture enables the delivery of emergency calls with highly-accurate location and caller information to PSAPs during an emergency anywhere in Europe. However, the use of PEMEA requires each entity to follow an **application approval procedure** which leads to the delivery of a certificate domain name and a label identifier allowed to indicate that it is PEMEA compliant.

The setup of such a procedure with new entities in a new frame work as proposed in PEMEA is a complex task. For this reason, it is planned in two phases:

- Phase I: bilateral agreements between PSPs. Here the approval process focuses on PSPs following the protocols and procedures to exchange information.
- Phase II: registration organisation is awarded, the ASP enabling the automatic routing is in place. Full registration process can occur.

The current revision of the document focuses on Phase I only.

2 Abbreviations and References

All definitions of terms and acronyms related to 112 are available in the 112 Terminology EENA Operations Document.¹ For convenience, they are also listed below.

2.1 Abbreviations

AP	Application Provider
App	Application
ASP	Aggregating Service Provider
CPE	Customer Premises Equipment
ERO	Emergency Response Organization
GNSS	Global Navigation Satellite System
MS	Member State
oPSP	Originating PSAP Service Provider
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
PSO	Public Safety Organization
SO	Strategic Objective
tPSP	Terminating PSAP Service Provider

2.2 References

- [1] EENA 2.2.3, "[112 Smartphone Apps](#)", an EENA Operations Document, February 2014
- [2] "[112 Apps Strategy - PEMEA](#)", an EENA Operations Document, March 2015
- [3] "[PEMEA Requirements and Functional Architecture](#)", an EENA Technical Document, December 2015
- [4] "[PEMEA Protocols and Procedures Specification](#)", an EENA Technical Document, April 2016

¹ www.eena.org/view/en/Committees/112operations/index/generalframework.html



3 PEMEA Application Approval

All entities, AP, PSPs, PSAPs and ASPs need to have a PEMEA identifier (PEMEA-ID) for compliancy purposes (PEMEA registration). The registration procedure described in this document is based on a trusted process dependent on peer sponsorship. That is, in order to operate as a PSP you must be sponsored by an established PSAP. To operate as an AP you must be sponsored by a PSP. This sets the initial stage for enrolment. All partners in this process already satisfy this requirement.

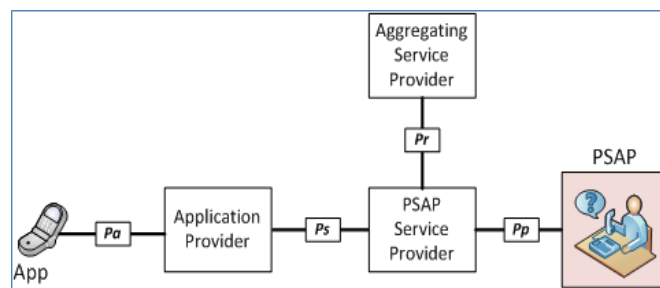


Figure 1 PEMEA Reference Architecture [R3]

In order to make the application approval procedure, a PEMEA registry is needed. In the following sections, this document describes the requirements for the PEMEA registry, what the registry provides to each of the identified PEMEA entities and finally a staged approach to implementing the PEMEA registry.

The primary goal of the PEMEA registry is to ensure that only trusted entities that comply with the PEMEA specifications are able to connect and deliver messages into the PEMEA network.

How the PEMEA registry achieves this is described in Section 3.1.

Implementation of the PEMEA registry is broken up into two phases that are described in Sections 3.2 and 3.3. The first phase establishes a manual process for the PEMEA registry to facilitate testing, piloting and implementations of a limited number of PEMEA entities.



3.1 Process Overview

In PEMEA **authentication** occurs before **authorization**. Authorization policies apply to specific entities, so the identity of the entity must first be verified.

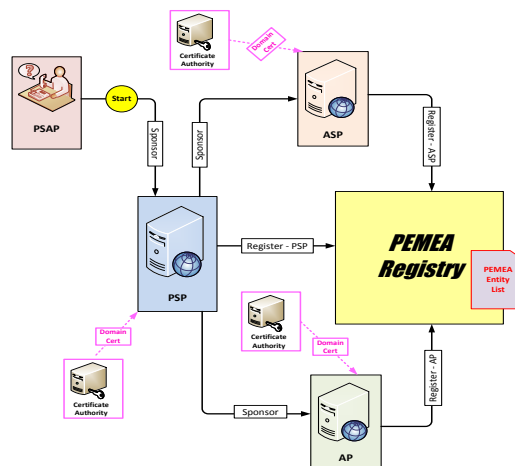


Figure 2 - Process overview

A PEMEA entity must be able to assert its identity to other PEMEA entities. It must do this when it wants to send data to another PEMEA entity, or when another PEMEA entity wishes to request information from it. Identity assertion in PEMEA is achieved using x.509v3 certificates².

A PEMEA entity therefore **MUST** have a certificate signed by a trusted public certificate authority and the certificate **MUST** allow then to:

1. Verify signature on certificates
2. Verify digital signature (used by servers to verify client identity assertions)
3. Key encipherment (used for private key exchanges)

Entities registering with PEMEA must secure an Internet domain name and must acquire a certificate with the above properties from a trusted public certificate.

Once this is obtained, then the registering entity supplies the following information to the PEMEA registration authority:

- Type of entity (AP, PSP, ASP, PSAP)
- Entity office contact details (country, entity name, entity address, primary contact person, contact details)
- Domain being registered
- Public certificate (this can be verified)
- Sponsoring entity (PSAP or PSP)

If this all checks out then the entity is provided a PEMEA-ID and is registered in the system.

It can then request a copy of the list (this is done through an HTTPS request where both the client and server mutually authenticate one another. This ensures that the list is always authentic).

² Refer to <https://tools.ietf.org/html/rfc6187>



3.2 Role of the PEMEA registry authority

The PEMEA registry authority is the institution responsible for the PEMEA program keeping the registry up to date. It processes the requests of different entities (i.e. AP/PSP) that wish to join the program and also oversees the acceptance delivery on the test certificate.

The registry update is performed via a PEMEA template in which the provider entity has to fill the required fields (refer to the table described in the section 5.3).

The test certificate is delivered according to a plug testing step performed against a reference configuration, namely PEMEA Testbed.

The provider entity that wants to join the program is assigned a technical specification document that describes the testing environment with the different parameters for Testbed connectivity as well as the test plan to achieve with the expected results. A testing windows is regularly set to allow the PEMEA registry entity to assist the provider entity in the testing execution.

Once the testing positively executed, the PEMEA registry authority delivers the PEMEA ID to the provider entity, then validates the registry and disseminates the update to the PEMEA community.

EENA will act as PEMEA registry authority during Phase I as an intermediate step.

3.3 Initial registration process

The initial registration process is designed to get PEMEA off the ground and allow interworking between early adopters. In the first instance, registration is expected to only be open to PSPs wanting to implement the **Pr interface (see figure 1)** to enable application roaming in other countries or regions.

PSP acquires a domain certificate and provides information to the PEMEA registration authority, including suitable evidence that it is a legitimate PSP. The specific information required is shown in Annex - Table 1.

Registrations shall be valid for a period of one year from the date of activation.

Languages are important because they vary widely across Europe; all support lines are expected to support at least one language beyond the native country language that is English.

Much of the information above is required for the PEMEA registry authority in order to help associate PEMEA entities to promote better coverage. Table 2 PEMEA entity list contains the information provided in the entity list downloaded by registered PEMEA entities to authorize other PEMEA entities.



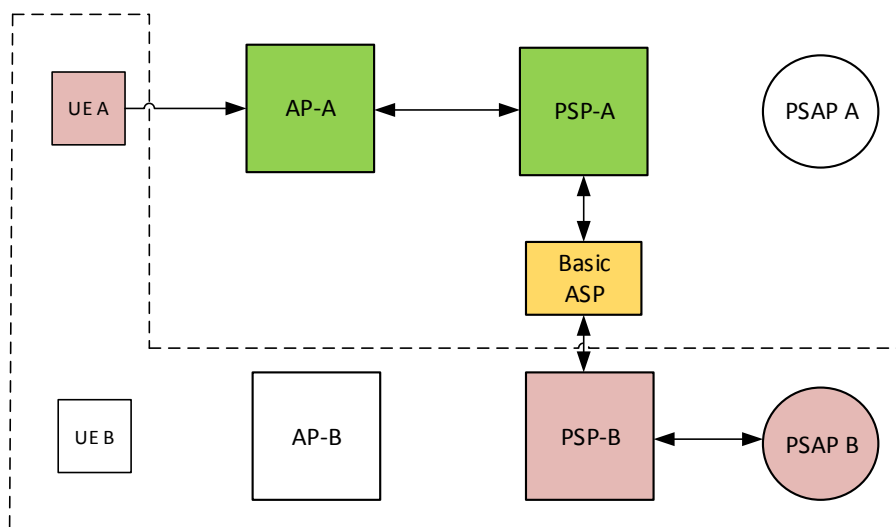
4 PEMEA Implementation process overview

4.1 Phase I process

The objective is to enable a first implementation of PEMEA. To illustrate the operation of this phase, we use, as an example, 2 PSPs that are located in two European countries: PSP-A in Austria and PSP-B in Belgium.

The principle is that each PSP in the first instance requires a certificate (domain name) and must obtain a mutual accreditation by each PSP.

Approval is recorded by the PEMEA Registry.



This solution allows an Austrian user to go to Belgium and have caller-data delivered to a Belgium PSAP.

The message flow in this case is UE--->PSP-Austria----->PSP-Belgium--->PSAP-Belgium

A basic ASP component is added to allow the protocol exchange running between PSP entities.

4.1.1 Implementation requirements overview

Here below is the list of requirements to fulfill to start the PEMEA implementation process Phase I

- Manual PEMEA registry authority operated by EENA.
- Preliminary entities registered with the manual PEMEA registry
- AP/PSP Early adopter's agreement template available
- A coordination technical team formed by Early Adopter companies

- A Basic ASP component will be deployed and available to allow data exchange. PSPs can also decide to do bilateral connections.
- Technical specification document which describe for AP/PSP the way to connect to the Testbed
- Test plan available for AP/PSP Early adopters to comment, provide input to, and to execute against.

4.1.2 PEMEA Entities role description

I'm a PSAP, what should I do?

- Contact and inform the registry authority (EENA) of willingness to be part of the program.
- May request assistance from registry authority in identifying the PEMEA entities (PSP) with whom you can perform interoperability testing.
- Provide the information from Table 1 to EENA
- Receive the PEMEA identity from EENA and an email of confirmation that the PSAP organization now belongs to the PEMEA community.

I'm a PSP, what should I do?

- Contact EENA for the requirements
- Acquire a domain name and an X.509 certificate from a well trusted certificate authority as proof of domain name ownership.
- Contact a registered PSAP and have them agree to sponsor you as their data provider. They must provide a brief notice of sponsorship that must include:
 - o The PSAP PEMEA-id
 - o PSAP personnel contact details
 - o Your registered domain name.
- Contact EENA, provide the PSAP sponsorship notice and your details from Table 1 to initiate the registration.
- EENA will check all details and will provide an interim PEMEA-ID to start the validation process. The tests will be made in order to ensure the PSP's compliancy with the PEMEA specifications.
- At the conclusion of testing a report indicating if you meet the criteria to connect to the wider PEMEA network. If the report is negative, then the PSP must address all outstanding issues prior to retesting.
- Once testing is complete and adherence agreed, EENA will finalize the allocated PEMEA-ID and add your details the registry file.
- At this point you will be provided with the complete PEMEA registered entity file. Other entities will be provided with an updated PEMEA registered entity file also, ensuring the interconnectivity is enabled.

4.1.3 End of phase I

The completion of phase I, will use the users' experience on the major changes to be implemented into the registry and operations process.

Also a specification update phase must be open to allow the integration of technical evolutions into the PEMEA specifications.

Clear and open test plans and specifications against which compliance is validated shall be available.



4.2 Phase II process

The objective will be to perform a live end-to-end testing phase with all currently specified PEMEA features available.

By completion of phase II a full PEMEA registry process is anticipated to be defined and implemented, along with a formal validation procedure for PEMEA functional entities. In addition to this an independent PEMEA registry organization should exist to manage the ongoing PEMEA registry activities. Trusts and authentication requirements

5 Conclusion

The intention of phase I of the PEMEA registry process is to implement interoperability between Emergency Apps in the short term by facilitating the exchange of data using the PEMEA registry information.

Feedback from this phase will be fed back into the overall PEMEA registry and operations process document for adopting into phase II that will become the content for a future revision of this document.



ANNEX

Table 1 PEMEA registration details

Num	Item	Description
1	Entity Name Language	The language that the entity name is specified in, this is a 2-digit country code, e.g. EN for English or DE for German.
2	Entity Name	The name of the entity.
3	Entity Address	The postal/street address of the entity.
4	Type of Entity	AP, PSP, ASP, PSAP (only PSP is expected at this time). Only one value is used. If an entity is a PSP, ASP and AP then it must have 3 entries, one for each.
5	Primary Contact Title Language	The language that the primary contact title is specified in, this is a 2-digit country code, e.g. EN for English or DE for German.
6	Title of Primary Contact	The position of the Primary Contact in the entity organization e.g. Director PEMEA data exchange.
7	First name of Primary Contact	First name of the Primary Contact, e.g. Susan.
6	Last Name of Primary Contact	Last name of the Primary Contact, e.g. McMurray.
8	Primary Contact Spoken Languages	A comma-separated list of 2-digit codes representing all languages spoken by the Primary Contact, e.g. EN for English or DE for German.
9	Primary Contact Written Languages	A comma-separated list of 2-digit country codes representing all languages read by the Primary Contact, e.g. EN for English or DE for German.
10	Email Address of Primary Contact	Email address of the Primary Contact. Emails may be expressed in any language listed as part of item 9.
11	Telephone number of Primary Contact	Voice calls may be made in any of the languages listed in item 8.
12	24 x 7 contact languages	A comma-separated list of 2-digit country codes representing all languages spoken by the 24 x 7 support staff, e.g. EN for English or DE for German.
13	24 x 7 Contact Number for entity support	In case of emergency a way to always be able to contact the entity.
14	Domain Name	The domain name that the entity asserts ownership over. This must match the subjectAltName in their x.509 certificate or all authorizations will fail.
15	Country of Operation (PSP, ASP or PSAP)	A comma-separated list of 2-digit country codes representing all countries in which the entity operates These must comply with ISO-3166-2 e.g. BE for Belgium or NL for The Netherlands. It is recommended that a separate registration for each country be made in case the Primary Contact or 24 x 7 Support details are different based on country.



16	Regions of Operation (PSP, ASP or PSAP)	In some cases an entity will not operate in all regions within a country. Where this is the case, the entity must indicate which regions it operates in. These must comply with ISO-3166-2, e.g. BE-BRU for Brussels-Capital Region or BE-VAN for Antwerpen province.
17	Activation Date	The date and time that the entity wishes the registration to become active.

Table 2 PEMEA entity list

Num	Item	Description
1	Type of Entity	One of: AP, PSP, ASP, PSAP.
2	Entity Name Language	The language that the entity name is specified in, this is a 2-digit country code, e.g. EN for English or DE for German.
3	Entity Name	The name of the entity.
4	24 x 7 contact languages	A comma-separated list of 2-digit country codes representing all languages spoken by the 24 x 7 support staff, e.g. DE,EN,FR for German, English and French.
5	24 x 7 Contact Number for entity support	In case of emergency a way to always be able to contact the entity.
6	Domain Name	The domain name that the entity asserts ownership over. This must match the subjectAltName in their x.509 certificate or all authorizations will fail.
7	PEMEA-ID	PEMEA issued Identifier unique for this entity.
8	Activation Date	The date the services activated.

