PEMEA CONSORTIUM

Connecting internet apps to emergency services

PEMEA Registration Authority Entities File Data

PEMEA-CONS-PRA-FILE-DATA

V1.0

27 Dec 2023

Contributors

Name	Company
James Winterbottom Miguel Ortega Adrián Mora Carrera Jorge Forcada	Deveryware

Table of Contents

1. Introduction ... 3
2. Terms and Definitions ... 3
3. Registering with the PRA ... 4
4. Retrieving the entities file data ... 5
5. Security ... 6
5.1 Entities file data retrieval ... 6
5.2 PRA management ... 6
6. Entities file data ... 7
6.1 Overview ... 7
6.2 Informative References ... 7
7. Application of the entities file to a PEMEA node ... 7
8. Abnormal behaviour of PEMEA nodes ... 8
8.1 PEMEA entity misbehaviour ... 8
8.2 PEMEA entity does not periodically download the entities file ... 8
9. References ... 9
9.1 Normative References ... 9
9.2 Normative References ... 9
ANNEX A Entity File JSON Schema ... 10
ANNEX B Cipher Suites ... 12
10. HISTORY ... 13

1. Introduction

The PEMEA Registration Authority (PRA) is a centralized node that maintains the contact and operator information for all valid PEMEA nodes in the PEMEA network. The PRA provides the valid PEMEA entities information to requesting valid PEMEA entities in an entities file data that each node needs to download on a periodic basis. This information is sensitive and under-pins the security and integrity of the PEMEA network, consequently, only valid nodes should have access to the information, and any node using the information needs to be sure that it is current and came from the PRA.

This document is intended for PEMEA system vendors, whose PEMEA nodes need to be able to contact the PRA, download the entities file data and subsequently process the information for use. It covers the procedures needed to acquire the entities file data, the structure and contents of the data, and how to correctly store and dispose the data. Ultimately, it is up to vendors and operators to ensure that contents of the entities file are not accessible outside of the scope of their systems.

2. Terms and Definitions

The following terms and definitions are used in this document:

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AESGCM	Advanced Encryption Standard key used with GCM
AP	Application Provider
ASP	Aggregating Service Provider
CA	Certificate Authority
DHE	Diffie-Hellman key Exchange
ECDHE	Elliptic-Curve Diffie-Hellman key Exchange
EDS	Emergency Data Send
EMTEL	Emergency Communications
ETSI	European Telecommunications Standards Institute
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IM	Instant Message
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
MAC	Message Authentication Code
PEMEA	Pan-European Mobile Emergency Application framework
PRA	PEMEA Registration Authority
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
RFC	Request for Comments
RSA	Rivest Shamir Adleman public key encryption algorithm
RTT	Real-Time Text

TLS	Transport Layer Security
TS	Technical Specification
URI	Uniform Resource Identifier
URL	Universal Resource Locator

3. Registering with the PRA

Each active PEMEA node needs to be registered with the PRA. This information is used by the PRA to:

1. Ensure that the entity has passed the relevant conformance tests required to join the PEMEA network.
2. Compose the valid PEMEA entities file data.
3. Authenticate the certificates of PEMEA entities requesting the entities file with against their registered domains as described in clauses 4 and 5.
4. Notify entities when network changes or issues are occurring.

The information required for any entity to register a node with the PRA are included in Table 1.

Table 1: Basic entity information

Information	Value	Description
Entity Type	One of: "AP", "PSP", "ASP", "PSAP"	The type of PEMEA node being registered.
PEMEA-ID	E.g. "urn:example:psp"	This is provided by the PRA to the registering entity.
Entity name	E.g. "Madrid 112"	Name of the entity registering the node.
Activation date	YYYY-MM-DD	This may be in the future. Activation occurs from midnight on the date specified.
Domain name	E.g. "psp.example.com"	The domain name to be used in the destination URI for the node. This must be unique across all PEMEA nodes.
Destination URI	E.g. "https://psp.example.com"	The HTTPS URI used to interact with this node. This is NOT required for AP nodes.
Contact languages	iso-639-1 alpha-2 language code. E.g. ["en", "es"]	Languages spoken by the entity's primary contact.
Contact number	E.g. "tel:+34636586999"	The tel URI for the primary contact that is operating the node.
Contact email	E.g. "primary.contact@psp.example.com"	The email address of the primary contact that is operating the node. The PRA sends relevant information to this email to inform about updates or misbehaviours in the network.

		If the same email is provided for more than one PEMEA nodes, the PRA only sends 1 notification to the entity's email, the entity shall update all their PEMEA nodes with the information received.

The PRA maintains a list of authorized PEMEA testing partners. Any registration must be accompanied by a compliance certificate from an authorized PEMEA testing partner.

Entities that are registering need to have their details contained in the PRA entities file data at least 24 hours prior to them coming online, this gives time for all nodes in the PEMEA network to download and apply the latest node.

4. Retrieving the entities file data

Each entity must download the entities file data periodically, it is recommended that this period should not be greater than every 24 hours. In the case that a PEMEA operator has multiple entities registered, he can make this download with one of the entities and update all the others. Only entities that are present in the valid entities file are allowed to download the entities file. Entities that are set with a future activation date are still permitted to download the entities file data. This ensures that they are ready to start sending and receiving requests once they go live.

Entities that are not active or do not have a future activation date are not permitted to connect to the PRA or to download the entities file data.

Entities requesting the entities file data are required to establish mutual authentication using x.509 certificates before a connection is established at the PRA. This means that each connecting node must have the PRA public domain certificate, or PRA's public root CA certificate in its trust store. The PRA validates the certificate of the node with the list of registered domains and only accepts requests with certificates issued for a registered domain.

The entities file is not really a file, but data. The structure of this data is defined in clause 6. Entities retrieve the entities file making an HTTPS request which require mutual TLS, and the PRA answer the requests with a body which has the entity file in JSON format.

The entities can store this data in a file or in a database, the details on how to store this data is left to the implementation, but the entities must ensure that the data is protected.

The URI for the PRA is https://pra.pemea.help, contact the PEMEA consortium for the root CA identity sending an email to pra@pemea.help.

The identity of the requesting node is recorded in the PRA along with the time the request was made and what information was provided to the entity. This ensures that the PRA knows which entities are up to date with their entity file data and which are not. This allows the PRA to notify non-conforming nodes ahead of being disabled for non-compliance of entity management.

Requests from the entities to the PRA to download the entities file must be made using mutual TLS certificate-based authentication, which is an extension of the TLS protocol that enables both the server and the client to authenticate each other using digital certificates. It adds an extra layer of security by requiring both parties to present valid certificates, ensuring that the server is communicating with the intended client and vice versa.

5. Security

5.1 Entities file data retrieval

The retrieval of the PRA entities file data is made using an HTTPS GET request described in clause 7.

The connection should preferably be made using TLS 1.3, though may be made using TLS 1.2.

Mutual TLS certificate-based authentication is required, nodes requesting the entities file should have the PRA root CA and domain name stored so that only requests answered with a certificate issued from a valid root CA for the domain name of the PRA are authenticated, and the PRA should have the node domain name in the registered domain names so that only requests requested with a certificate issued from a valid root CA for the domain name of the requesting node are authenticated.

This ensures that the connection to the PRA is secured and authenticated.

The entities file is sent from the PRA to the requesting node over the secure TLS connection, the requesting node should store the information ensuring that the data is protected.

The lists for the TLS 1.3 and TLS 1.2 acceptable cipher suites are included in ANNEX B.

5.2 PRA management

Besides the entities file retrieval, the PRA has other management operations that can only be made by authenticated users. These users will login into the PRA using a username and password provided by the PRA managers. Each user has one role and only can manage certain data inside the PRA.

- Administrator users are able to:
    - Create PRA users.
    - Remove PRA users.
    - Manage PRA user usernames and password.
- Operator users are able to:
    - Create PEMEA entities.
    - Change PEMEA entities.
    - Activate PEMEA entities.
    - Deactivate PEMEA entities.
- Auditor users are able to:
    - Retrieve the logs of all the operations that have taken place in the PRA.

6. Entities file data

6.1 Overview

The retrieval of the PRA entities file data is made using an HTTPS GET request from the requesting entity to the PRA with the path /pemea/entities.

The entities file is a JSON document that contains a list of all the entities that are either active or have a future activation date. If an entity is not in the list, then it is not a valid PEMEA entity, even if it has been in the past. The JSON schema for this entities file is provided in ANNEX A.

It is delivered only to requesting entities following the security described in clause 5.

6.2 Informative References

The general structure of the file is show in Table 2.

Table 2: Entities file entity data

Element	Description
pemeaId	PEMEA-ID of the node.
type	The type of PEMEA node; AP, PSP, ASP, PSAP.
domainName	The domain of the node; this is expected to be the same as the x.509 subjectAltName field.
url	The URL used to connect to the node. This value may be null for an AP. The domain name component of this URL shall be the same as the domain name field.
activationDate	The date that the node came, or is coming, online.
name	Name of the entity that is operating the node.
languages	The languages spoken by the entity that is operating the node.
phoneNumber	The phone number for the primary contact that is operating the node.
email	The email address of the primary contact that is operating the node.

An example file with one entry is provided below.

```
[
  {
    "pemeaId": "urn:ees:pemea:spain:develop:asp",
    "type": "ASP",
    "domainName": "asp.pemea.es",
    "url": "https://asp.pemea.es/pemea",
    "name": "ASP de España",
    "languages": ["ES"],
    "phoneNumber": "+34612345678",
    "email": "pemea.spain@gmail.com",
    "activationDate": "2022-03-06T10:52:48.906472+11"
  }
]
```

7. Application of the entities file to a PEMEA node

To receive an entities file, a PEMEA node shall:

1. Make the GET request to the PRA described in clause 5 taking into consideration the security measures described in clause 6.
2. Parse the data received against the schema provided in ANNEX A.

If this is the first time that the PEMEA node is applying an entities file, then the entities file may be loaded at this point providing steps 1 and 2 have successfully passed.

If the PEMEA node has already had an entities file loaded, then the new entities file shall be loaded.

If the date of the just received entities file is equal to or lower to the previously applied entities file, then the new entities file shall be discarded.

8. Abnormal behaviour of PEMEA nodes

8.1 PEMEA entity misbehaviour

If a valid PEMEA entity is misbehaving and it is detected by another PEMEA entity, the operators of the PEMEA node that is detecting the bad behaviour must communicate this to the PRA operators. This can be done contacting to the PEMEA consortium and providing the information about the abnormal behaviour detected from the misbehaving PEMEA entity.

PRA operators will check the information delivered by the entity and disable the misbehaving PEMEA node in the entities file. An email is sent to all PEMEA nodes to warn them that the file has changed so that PEMEA nodes can retrieve the new entities file and update the information, which includes the disabled PEMEA node.

PRA operators will check the information delivered by the entity reporting the misbehaviour and will deactivate the PEMEA entity in the entities file, and will send an email to the email address that PEMEA entities provided when registering in the PRA warning that an update in the PRA entities file has occur and that they should update the entities file to apply the new update.

PRA operators will use the contact information provided by the misbehaving PEMEA entity to contact the agency responsible of the PEMEA entity to warn them that their PEMEA node has been disabled.

8.2 PEMEA entity does not periodically download the entities file

If the PRA detects that a registered and activated PEMEA entity has not requested the PEMEA file in 48 hours, it will send an email to the email address provided by the PEMEA entity when it was registered in the PRA warning that if it does not retrieve the PRA entities file in 2 hours, it will be deactivated.

If the 2 hours pass and the PEMEA entity has not yet downloaded the entities file, the PRA will:

1. Automatically deactivate the PEMEA entity.
2. Send an email to the PEMEA entity warning that it has been deactivated.

3. Send an email to all registered PEMEA entities warning them that an update in the PRA entities file has occur and that they should update the entities file to apply the new update.

A PEMEA operator that manages more than one PEMEA entity can retrieve the entities file data only with one of his nodes and then moving internally the information to the other entities he operates. In this case, the email provided from the PEMEA operator will be used as unique identifier. The PRA will consider that if one of the nodes associated with an email have updated, the other nodes managed by that associated email are updating the PRA entities file data too.

9. References

9.1 Normative References

[R.1] ETSI TS 103 478: “Emergency Communications (EMTEL); Pan-European Mobile Emergency Application”, March 2020.

[R.2] IETF RFC 6750: “The OAuth 2.0 Authorization Framework: Bearer Token Usage”, October 2012.

[R.3] IETF RFC 2617: “HTTP Authentication: Basic and Digest Access Authentication”, June 1999.

9.2 Normative References

ANNEX A Entity File JSON Schema

```
    "definitions": {},
    "$schema": "http://json-schema.org/draft-07/schema#",
    "$id": "https://ghale.help/schemas/pra/pra.json",
    "title": "PRA Schema",
    "type": "array",
    "description": "PRA schema definition of active PEMEA Entities",
    "items": {
        "type": "object",
        "title": "PRA Entity Schema",
        "required": [
            "pemeaId",
            "type",
            "domainName",
            "name",
            "languages",
            "phoneNumber",
            "email",
            "activationDate"
        ],
        "properties": {
            "pemeaId": {
                "type": "string",
                "title": "The PEMEA ID",
                "minLength": 1,
                "pattern": "^urn(?::[a-zA-Z-0-9]+)+$",
                "examples": [
                    "urn:ees:pemea:deveryware:ap"
                ]
            },
            "type": {
                "type": "string",
                "title": "The entity type",
                "enum": ["AP", "PSP", "ASP", "PSAP"]
            },
            "domainName": {
                "type": "string",
                "title": "The domain name of the entity",
                "pattern": "^[a-zA-z0-9-]+(?:\\.[a-zA-Z0-9-]+)+$",
                "examples": [
                    "ap.ghale.help"
                ]
            },
            "url": {
                "type": "string",
                "title": "The entity URL to send EDS to",
                "pattern": "^https://[a-zA-z0-9-]+(?:\\.[a-zA-Z0-9-]+)+(?::[0-
9]+)?(?:/[a-zA-Z0-9-]+)*/?$",
                "examples": [
                    "https://psap.ghale.help/pemea"
                ]
            },
            "name": {
                "type": "string",
                "title": "The name of the entity",
                "minLength": 1
            },
            "languages": {
                "type": "array",
                "description": "The list of acceptable languages abbreviations.
Abbreviations must match IANA language subtag registry.
http://www.iana.org/assignments/language-subtag-registry/language-subtag-registry",
                "uniqueItems": true,
                "items": {
                    "type": "string"
                }
            },
            "phoneNumber": {
                "type": "string",
                "title": "The contact number to call for critical issues",
                "pattern": "^\\+[0-9]+$",
                "minLength": 3,
                "examples": [
                    "+34666554433"
                ]
            },
            "email": {
                "type": "string",
                "format": "email",
                "minLength": 5,
                "examples": [
                    "info@info.com"
                ]
            },
            "activationDate": {
                "type": "string",
                "title": "The UTC timestamp of when the entity will be active",
                "pattern": "^[0-9]{4}(?:-[0-9]{2}){2}T[0-9]{2}(?::[0-9]{2}){2}Z$",
                "minLength": 1,
                "examples": [
                    "2018-11-06T15:48:56Z"
                ]
            }
        }
    }
}
```

ANNEX B Cipher Suites

This annex provides a recommended set of cipher suites for use with this protocol.

Table B.1: Recommended TLS 1.3 cipher suites

Cipher	TLS version	Encryption	MAC
TLS_AES_128_GCM_SHA256	1.3	AESGCM(128)	AEAD
TLS_AES_256_GCM_SHA384	1.3	AESGCM(256)	AEAD
TLS_CHACHA20_POLY1305_SHA256	1.3	CHACHA20/POLY1305(256)	AEAD

Table B.2: Acceptable TLS 1.2 cipher suites

Cipher	TLS version	Encryption	MAC
ECDHE-ECDSA-AES128-GCM-SHA256	1.2	AESGCM(128)	AEAD
ECDHE-RSA-AES128-GCM-SHA256	1.2	AESGCM(128)	AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	1.2	AESGCM(256)	AEAD
ECDHE-RSA-AES256-GCM-SHA384	1.2	AESGCM(256)	AEAD
ECDHE-ECDSA-CHACHA20-POLY1305	1.2	CHACHA20/POLY1305(256)	AEAD
ECDHE-RSA-CHACHA20-POLY1305	1.2	CHACHA20/POLY1305(256)	AEAD
DHE-RSA-AES128-GCM-SHA256	1.2	AESGCM(128)	AEAD
DHE-RSA-AES256-GCM-SHA384	1.2	AESGCM(256)	AEAD

10. HISTORY

Document history		
V1.0	27 Dec 2023	First stable version.
V0.6	15 Sep 2023	Rename file. Update procedure to consider a PEMEA node as not being periodically downloading updates.
V0.5	29 May 2023	Clarify definition of PRA file. Remove personal information from entities file delivered to PEMEA nodes.
V0.4	21 November 2022	Fixed formatting
V0.3	17 November 2022	Updated with corrected schemas
V0.2	9 November 2022	Updated with comments
V0.1	8 November 2022	Initial Draft