

# Public Key Infrastructure (PKI)

*Telematics TSI - Technical document - 106*

*Version 4.0*

## Contents

A.	Document management .....	6
A.1	Document properties .....	6
A.2	Change management .....	6
A.3	Configuration management .....	6
A.4	Availability .....	6
A.5	Application and actors in the scope .....	6
A.6	Document history .....	6
B.	Acronyms, definitions and external references .....	8
B.1	Acronyms .....	8
B.2	Definitions .....	9
B.3	External references .....	9
1.	Definitions and acronyms .....	11
2.	References .....	11
3.	Introduction .....	11
4.	Scope .....	11
5.	PKI schema .....	12
5.1.	PKI infrastructure and participating actors .....	12
5.1.1.	Requesting undertaking .....	13
5.1.2.	Certification authorities (CA) .....	13
5.1.3.	Registration authorities (RA) .....	13
5.1.4.	Validation authorities (VA) .....	13
5.1.5.	Subscribers .....	13
5.2.	Uses cases .....	13
5.2.1.	Communications .....	13
5.2.2.	Access to reference files and databases .....	14
5.2.3.	Ticketing .....	14
6.	Qualification of Certification Authorities .....	15
7.	Certification chain .....	15
7.1.	Organisation certification chain .....	17
7.1.1.	Certificate requirements .....	18
7.2.	PKI architecture .....	18
7.2.1.	Architectural requirements for the organisation certificate ORCAC for RA/CA .....	19
7.2.2.	Architectural requirements for other CA/RA .....	19
7.3.	Publication and repository responsibilities .....	19
7.3.1.	Repositories .....	19
7.4.	Identification and authentication .....	19
7.4.1.	Initial identification .....	19
7.4.2.	Subsequent identification .....	19
7.5.	Naming .....	20
7.6.	Initial identity validation .....	20
7.6.1.	Identity verification for organisations .....	20
7.6.2.	Identity verification RU/IM, RU/RU, RU/WK communication .....	20

7.6.3.	Identity verification ticketing .....	20
7.7.	Identification and authentication for re-key requests.....	20
7.8.	Identification and authentication for revocation request .....	21
8.	Certificate life-cycle operational requirements.....	22
8.1.	Organisation Certificate Application.....	22
8.1.1.	Organisation certificates.....	22
8.1.2.	RU/IM, RU/RU, RU/WK certificates .....	22
8.1.3.	Ticketing certificates .....	22
8.2.	Certificate application processing.....	22
8.2.1.	Organisation certificate (ORCAC) application .....	22
8.2.2.	Other certificates (ONCC, OSCC, OTAC, PTDAC) .....	22
8.3.	Certificate issuance .....	22
8.4.	Certificate acceptance .....	22
8.5.	Key pair and certificate usage.....	22
8.6.	Certificate renewal.....	22
8.6.1.	Organisation certificates.....	23
8.6.2.	RU/IM, RU/RU, database access certificates .....	23
8.6.3.	Ticketing certificates .....	23
8.6.3.1.	Exchange of certificates with partner companies .....	24
8.7.	Certificate re-key.....	24
8.8.	Certificate modification .....	24
8.9.	Certificate revocation and suspension .....	24
8.10.	Certificate status services .....	24
9.	Certificate, CRL and OCSP profiles .....	24
9.1.	Certificate profile .....	24
9.1.1.	Operator profile .....	24
9.1.2.	Operator Non-Safety Communication (ONCC) profile.....	25
9.1.3.	Operator Safety Communication (OSCC) profile .....	25
9.1.4.	Operator ticketing Certificate .....	25
9.2.	CRL profile .....	26
Annex I –	Organisational requirements for a Certification Authority .....	27
1.	Context of the Organization.....	28
1.1.	Understanding the Organization and Its Context .....	28
1.1.1.	Identify stakeholders and understand the regulatory, operational, and technical environments.....	28
1.1.2.	Define services including certificate issuance for railway systems. ....	28
1.2.	Understanding the Needs and Expectations of Interested Parties.....	28
1.2.1.	Document legal, regulatory, and contractual obligations. ....	28
1.2.2.	Address sector-specific requirements. ....	28
1.3.	Determining the Scope of the CA's Trust Services.....	28
1.3.1.	Define scope in CP/CPS including certificate types and assurance levels. ....	28
2.	Leadership.....	28
2.1.	Leadership and Commitment .....	28
2.1.1.	Ensure senior management commitment and alignment with applicable ETSI, ISO, EC standards. ....	28

2.2.	Policy .....	28
2.2.1.	Define an information security and trust service policy. ....	28
2.3.	Roles, Responsibilities, and Authorities .....	28
2.3.1.	Define roles, ensure role segregation, and maintain job descriptions. ....	28
3.	Planning .....	28
3.1.	Actions to Address Risks and Opportunities .....	28
3.1.1.	Conduct risk assessments and establish response procedures. ....	28
3.2.	Objectives and Planning to Achieve Them.....	28
3.2.1.	Define measurable objectives and KPIs. ....	28
3.3.	Planning for Change .....	28
3.3.1.	Apply change management and inform stakeholders. ....	28
4.	Support .....	28
4.1.	Resources .....	28
4.1.1.	Ensure adequate resources (e.g., staff, infrastructure). ....	28
4.2.	Competence .....	28
4.2.1.	Hire, train, and evaluate qualified personnel. ....	28
4.3.	Awareness.....	28
4.3.1.	Ensure staff understand policies and responsibilities. ....	28
4.4.	Communication.....	28
4.4.1.	Maintain clear internal and external communication channels. ....	28
4.5.	Documented Information .....	28
4.5.1.	Maintain and control all operational and compliance documents.....	29
5.	Operations .....	29
5.1.	Operational Planning and Control .....	29
5.1.1.	Manage certificate lifecycle and secure cryptographic operations.....	29
5.2.	Outsourced Processes.....	29
5.2.1.	Control third-party providers through SLAs and audits.....	29
5.3.	Change Management.....	29
5.3.1.	Authorize and document operational changes. ....	29
5.4.	Security Controls Implementation.....	29
5.4.1.	Enforce physical, logical, and system security measures. ....	29
6.	Performance Evaluation.....	29
6.1.	Monitoring, Measurement, Analysis, and Evaluation.....	29
6.1.1.	Monitor KPIs, maintain logs, and evaluate security events.....	29
6.2.	Internal Audit .....	29
6.2.1.	Conduct regular audits of CA operations and compliance. ....	29
6.3.	Management Review .....	29
6.3.1.	Review audit results, incidents, and performance indicators. ....	29
7.	Improvement .....	29
7.1.	Risks and mitigating measures.....	29
7.1.1.	Document the contribution of risk assessment to the overall CA performance improvement .....	29
7.2.	Nonconformity and Corrective Action .....	29
7.2.1.	Document and resolve non-conformities with root cause analysis. ....	29
7.3.	Continual Improvement.....	29

7.3.1. Use feedback and assessments to improve trust services. .... 29

Annex II – Technical requirements ..... 30

1. For Certification/Registration authorities..... 30

2. For PKI clients..... 32

## A. Document management

### A.1 Document properties

- File name: ERA\_TD\_106.docx
- Subject and document type: Telematics TSI - Technical document - 106
- Author: European Railway Agency
- Version: 4.0

### A.2 Change management

Updates to this technical document shall be subject to Change Control Management procedure managed by the Agency pursuant:

- the applicable requirements in the reference TSI
- Art. 23(2) of the Agency Regulation

If necessary, working groups are created in line with Art. 5 of the Agency Regulation.

### A.3 Configuration management

A new version of the document will be created if new changes are considered following the Change Control Management Process led by ERA.

More specifically:

- if there is a change in the requirements which influences the implementation
- if information is added to or deleted from the technical document
- adding test cases to the field checking in messages or databases.

Modifications will have to be highlighted, so they can be easily identified.

Disclaimer:

Specific legal references to technical documents and legal acts shall be revised after the enter into force of the Telematics TSI. In some sections this text can be highlighted.

### A.4 Availability

The version in force of this document is available on Agency's Gitlab repository. Any printed copy is uncontrolled.

### A.5 Application and actors in the scope

Date of entry into force of reference TSI.

This document applies to all the actors in the scope of the reference TSI.

### A.6 Document history

Table 1 - Document history

<i>Version</i>	<i>Date</i>	<i>Comments</i>
0.1	20/12/2024	Initial version
0.2	17/04/2025	Version for consultation

0.3	12/05/2025	Revision following comments
0.4	15/05/2025	2nd revision following comments from XLS
0.5	16/05/2025	3rd revision following the 15/05
4.0	10/06/2025	Initial version for Telematics TSI

## B. Acronyms, definitions and external references

### B.1 Acronyms

Table 2 – Acronyms

<i>Abbreviation</i>	<i>Full text</i>
CA	Certification Authority
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CER	The Community of European Railway and infrastructure companies
DN	Distinguished Name
EC	European Commission
EEA	European Economic Area
EEC	European Economic Community
EIM	European Rail Infrastructure Managers
EN	European standard
ERA	European Union Agency for Railways also called “the Agency”
ESO	European Standardisation Organisation
EU	European Union
IM	Infrastructure Manager
INF	Infrastructure
ISO	International Organisation for Standardisation
MS	EU or EEA Member State
NSA	National Safety Authority
NSR	National Safety Rule
NTR	National Technical Rule
ONCC	Operator non-safety communication certificate
PKI	Public Key Infrastructure
RA	Registration Authority
RFU	Recommendation for Use
RISC	Railway Interoperability and Safety Committee
RU	Railway Undertaking
SC	Standard Committee
TR	Technical Report
TS	Technical Specification
TSI	Technical Specification for Interoperability
TV	Ticket vendor



<i>Abbreviation</i>	<i>Full text</i>
UIC	International Union of Railways (Union Internationale des Chemins de Fer)
UIP	International Union of Private Wagons Owners (Union Internationale d'associations de Propriétaires de wagons de particuliers)
UIRR	International Union of Combined Road–Rail Transport Companies (Union Internationale des opérateurs de transport combiné Rail-Route)
UITP	International Association of Public Transport (Union Internationale des Transports Publics)
UNIFE	Union of the European Railway Industries (Union des Industries Ferroviaires Européennes)
WG	Working Group
WP	Working Party

## B.2 Definitions

Terms contained in this document are defined in the ERA Ontology. Specific definitions are below.

<i>Terms</i>	<i>Definition</i>
Public Key Infrastructure (PKI)	<p>A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.<sup>1</sup></p> <p>It implements the functions of Certification Authority, Registration Authority and Validation Authority. Those functions can be distributed or centralized.</p>

## B.3 External references

The referenced documents listed in Table 2 are indispensable for the application of this document:

- **For dated references, only the edition cited applies;**
- **For undated references, if any, the latest edition of the referenced document (including any amendments) applies.**

Table 2 Reference documents

<i>Id</i>	<i>Title</i>	<i>Doc ID, Edition</i>	<i>Date</i>	<i>Author/ Publisher</i>
[1]	Directive 2012/34/EU of The European Parliament and of The Council establishing a single European railway area.	Directive 2012/34/EU	21/11/2012	EC
[2]	Directive (EU) 2016/797 of the European Parliament and of the council of 11 May 2016 on the interoperability of the rail system within the European Union (Recast)	Directive (EU) 2016/797	11/06/2016	EC

<sup>1</sup> [https://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](https://en.wikipedia.org/wiki/Public_key_infrastructure)

[3]	Commission implementing regulation (EU) 2019/773 of 16 May 2019 on the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system within the European Union and repealing Decision 2012/757/EU	Commission implementing regulation (EU) 2019/773	08/09/2023	EC
[4]	Commission Implementing Regulation - TSI Telematics			EU
[5]	Commission Implementing Decision (EU) 2018/1614 of 25 October 2018 laying down specifications for the vehicle registers referred to in Article 47 of Directive (EU) 2016/797 of the European Parliament and of the Council and amending and repealing Commission Decision 2007/756/EC	Commission Implementing Decision (EU) 2018/1614	25/10/2018	EU
[6]	ERA-TD-103	ERA_Technical_Document_TAF-TD-103.pdf	XXX	ERA
[7]	ERA-TD-104	ERA_Technical_Document_TAF-TD-104.pdf	XXX	ERA
[8]	ERA-TD-105	ERA_Technical_Document_TAF-TD-105.pdf	XXX	ERA
[9]	ERA-REC-122/TD/02 – version 2 - Digital security elements for rail passenger ticketing	ERA-TD-TAP_B12	XXX	ERA
[10]	Technical Interface Specifications – Cybersecurity SP-SEC-ServSpec	<a href="#">Version 1.0</a> SP-SEC-ServSpec -V1.0 - February 2025.pdf	February 2025	Europe's rail
[11]	RFC 4211 „Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)“		2005	
[12]	RFC 6712 „Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol (CMP)“,		2012	

## 1. Definitions and acronyms

See section B.1

See section B.2.

## 2. References

See section B.3.

## 3. Introduction

A Public Key Infrastructure (PKI) is a set of processes, policies, and technology for associating asymmetric cryptographic keys with the entity to whom those keys were issued. It is a standardized method used for authentication and encryption to confirm the identity of communicating parties as well as validate information being shared. It can contribute to implement the three main pillars of information security: confidentiality, integrity and availability.

According to Article 8 “Common central repository and reference data” of the Telematics TSI, measures shall be implemented to ensure the cybersecurity of the Telematics TSI.

The European Union Agency for Railways shall make publicly available the reference data on their website. A common central repository shall be set-up for the provision of those data to support the implementation of the telematics TSI. One part of the repository shall include the list of certification authorities for the public-key infrastructure. This is relevant to set-up and operate a public-key infrastructure PKI. This PKI is used to secure the communication between the telematics stakeholders, then authentication against the databases and the security certificates for ticketing. The central repository shall follow the principles of an PKI.

## 4. Scope

This document describes the setup of the public key infrastructure (PKI), used for the TSI telematics. It is based on the document “Shared Cybersecurity Services Specification [10]”, applicable for all TSIs subject to requirements for cybersecurity.

The technical document PKI refers to the specific requirements concerning the setup of a PKI for the telematics TSI. Functions specified in [10], but not being relevant for the implementation of the telematics TSI, will not be referred to in this document.

## 5. PKI schema

The coverage of the description of the usage of digital certificates issued under the PKI scheme described in this document is limited to the scope of the Telematics TSI. Further functions can be included depending on specific change requests.

### 5.1. PKI infrastructure and participating actors

A Public Key Infrastructure (PKI) is a set of processes, policies, and technology for associating asymmetric cryptographic keys with the entity to whom those keys were issued. It is a standardised method used for authentication and encryption to confirm the identity of communicating parties as well as validate information being shared.

The PKI manages X.509 Digital Certificates, a type of certificate that includes information about the identity of the owner, a digital signature from the certificate authority, and a public key for encryption of data or validation of signatures. It's important to note that the private key, which is not included in the certificate, is required for decryption of data or creating signatures. The PKI manages those certificates.

This chapter describes the identity or types of entities that fill the roles of participants within the telematics PKI. The overall architecture of the roles of the PKI is explained in the architecture in Figure 1 – .

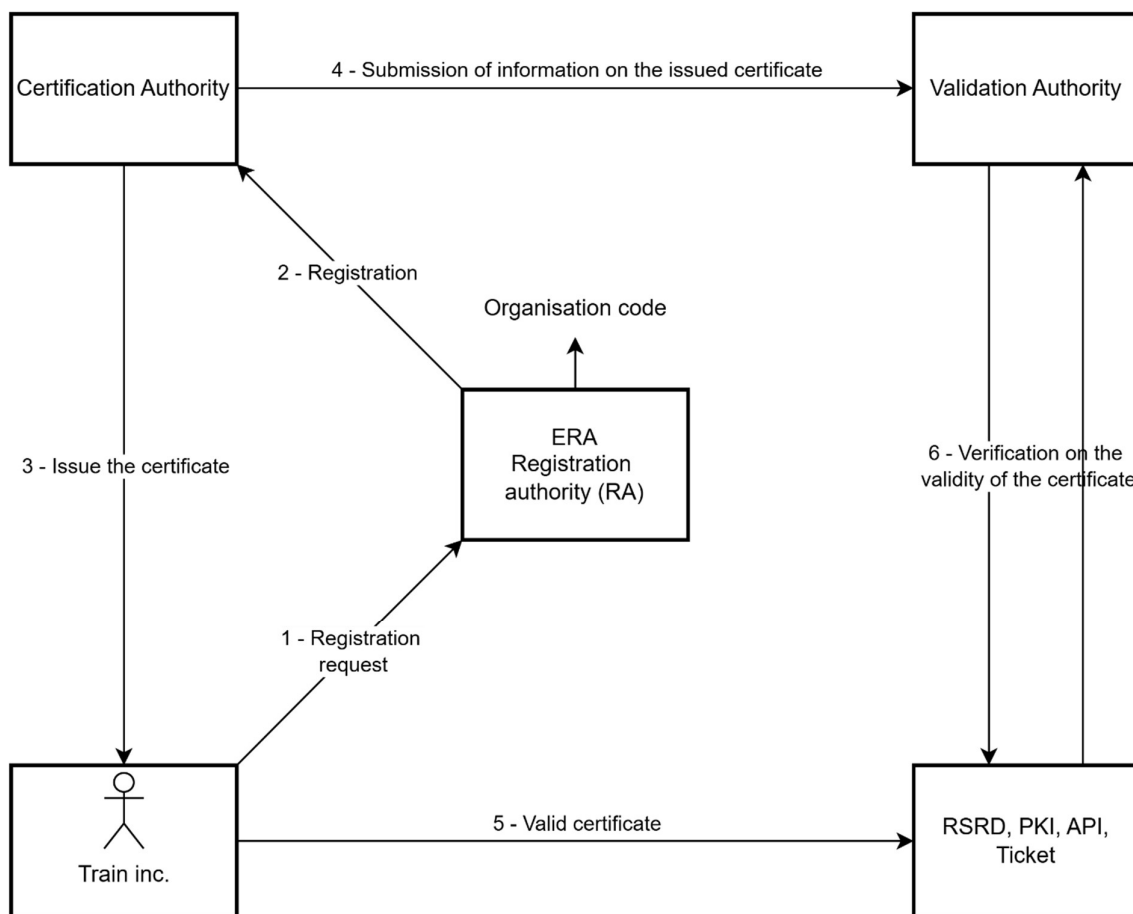


Figure 1 – Public Key Infrastructure

The following roles are addressed by the PKI for telematics applications:

#### 5.1.1. *Requesting undertaking*

Any telematics stakeholder as defined in Art 3(9) of the Telematics TSI, can use certificates issued by a CA, after the Registration Authority has registered the entity, for validation of the entity identity (i.e. authentication) against a Validation Authority.

Other actors are not entitled to receive a certificate to be used for the telematics applications. An organisation certificate might be used for several purposes.

The certificates to be used are public certificates to check the identity of the certificate holder.

#### 5.1.2. *Certification authorities (CA)*

In the Public Key Infrastructure, a Certification Authority is an entity responsible for issuing digital certificates used to verify the identity of entities and to facilitate secure communication over networks.

ERA sets out the organisational and technical requirements to qualify the Certification Authorities. Once qualified the CA details will be published by ERA.

#### 5.1.3. *Registration authorities (RA)*

The registration authority is registering the entities taking part in the key exchange. They are responsible for the enrolment procedures for organisation certificates, and they perform the identification and authentication of certificate applicants, initiate, or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA.

The role of the registration authority for organisation certificates is assigned to ERA.

#### 5.1.4. *Validation authorities (VA)*

The validation authority provides information about the validity of certificates. This can be ensured via access to Certificate Revocation Lists (CRL). In this PKI schema, the role of CA and VA will be fulfilled by the same organisation.

#### 5.1.5. *Subscribers*

In a Public Key Infrastructure (PKI), a subscriber is typically an entity (such as a person, organization, a device or a local PKI) that is issued a digital certificate by a Certificate Authority (CA). This digital certificate contains the subscriber's public key and other identifying information.

## 5.2. **Uses cases**

The scope of this PKI schema includes:

#### 5.2.1. *Communications*

For the communications purpose, the certificates shall be used to:

- authenticate different participants in communications under the scope of the Telematics TSI, implemented as machine-to-machine communications, and
- to encrypt the contents of those communications. Encryption of messages is mandatory when they are sent over the public network.

The participants in those communications can be Application Programming Interface implementing machine-to-machine communications or systems used for the exchange of datasets and messages for retail functions (e.g. ticketing).

The certificates shall ensure that the communication between both parties can be trusted, as required by the chapter 1.3. Cybersecurity of the Telematics TSI - Annex.

This comprises the certificates to be used to access the common interface according to ERA-TD-104 [7].

### 5.2.2. Access to reference files and databases

To access the reference files (if not public) and databases according to ERA-TD-103 [6], certificates shall be used to authenticate the users against those databases. The certificates shall ensure that only authenticated users can access the databases, as required by the chapter 1.3. Cybersecurity of the Annex I of the Telematics TSI.

### 5.2.3. Ticketing

To check the validity of the security elements (e.g. barcodes) for ticketing, certificates shall be used to identify who has issued those tickets and that the content of the security elements is unchanged.

This comprises the public certificates to be used to create the security elements according to and ERA-TD -B12) [9].

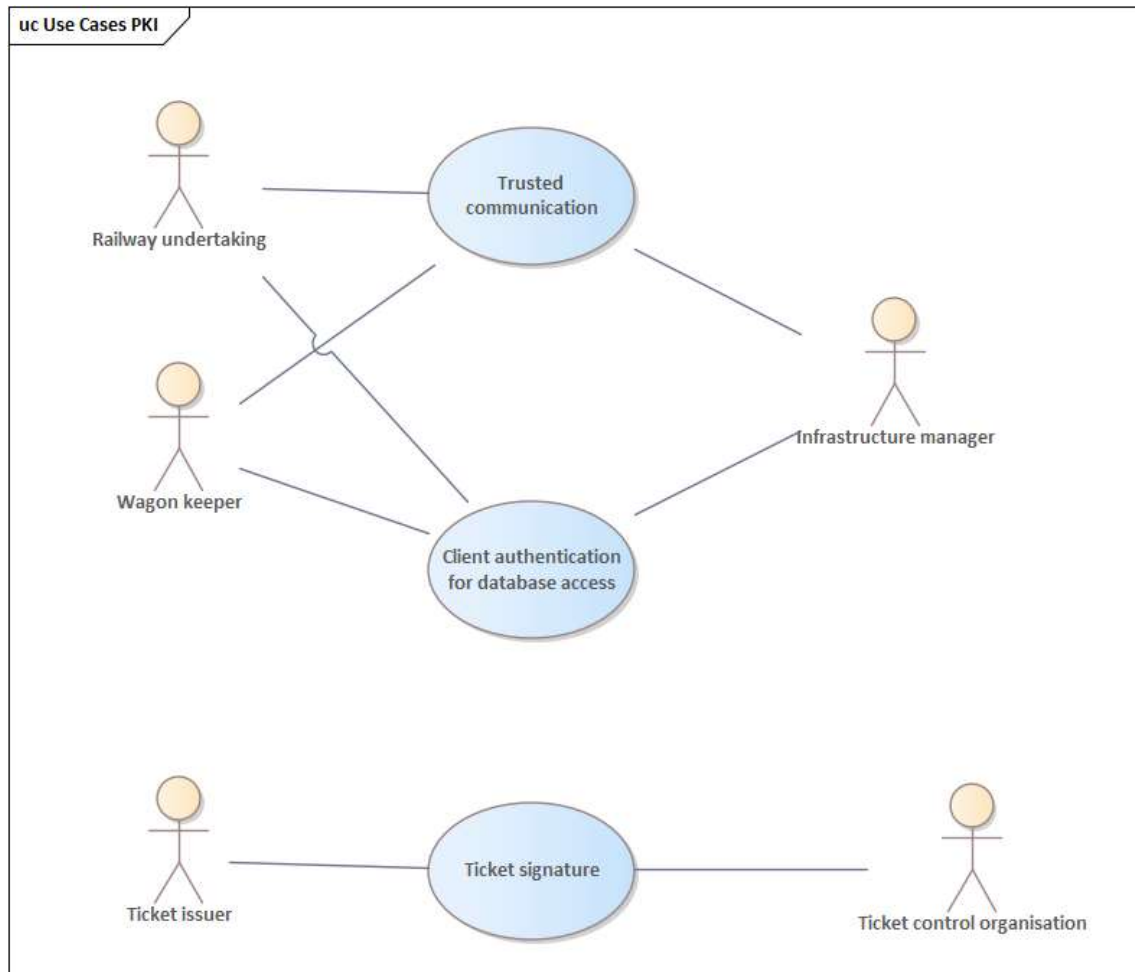


Figure 2 - use cases for certificates

The certificates used for the telematics applications are then limited to the following functions:

1. encrypted the trusted communication between the actors (e.g. via common interface, reservation systems, electronic consignment note);
2. the client certificates used for the authentication used for the access to the various databases (e.g. RSRD);
3. the signature of the security elements used for ticketing;
4. the signature used for electronic consignment note.

More specifically, the certificates issued by the organisations can be used for the following use cases:

1. RU/IM communication, via APIs
2. RU/RU communication, via APIs
3. IM/IM communication, via APIs
4. RU/WK communication, via APIs
5. WK/WK communication, via APIs
6. Access to common databases, via APIs
7. Ticketing certificates for electronic tickets
8. Electronic consignment note.

Any other usage for other purposes, such as for website certificates or the authentication for financial processes are not permitted.

## 6. Qualification of Certification Authorities

In line with Art. 8 of Telematics TSI, the Agency has to make available via the common central repository a list of Certification Authorities for Public Key Infrastructure ('PKI').

To be part of the repository, the PKI Certification Authorities will have to satisfy:

- The organisational requirements set out in Annex I.
- The technical requirements set out in Annex II.

## 7. Certification chain

The overall architecture of the certification chain for telematics shall be established as a hierarchical structure. The hierarchy is described in Figure 3.

The key principle of the PKI is to issue an organisation root certificate (ORCAC) by a CA listed in the Agency's common central repository for any organisation subject to the telematics TSI.

The CA will sign these certificates by a publicly recognised certificate, issued by a public CA.

The Agency will publish these certificates.

Based on the organisation root certificate the organisations can issue sub certificates for the different use cases addressed in the telematics TSI.

**Organisations can also decide to rely on other's PKI based on certificates issued by CAs published on the Agency repository, playing the role of Registration Authority (Figure 4)**

To obtain an intermediate certificate, the organisation will have to have a Organisation Code, assigned by ERA.

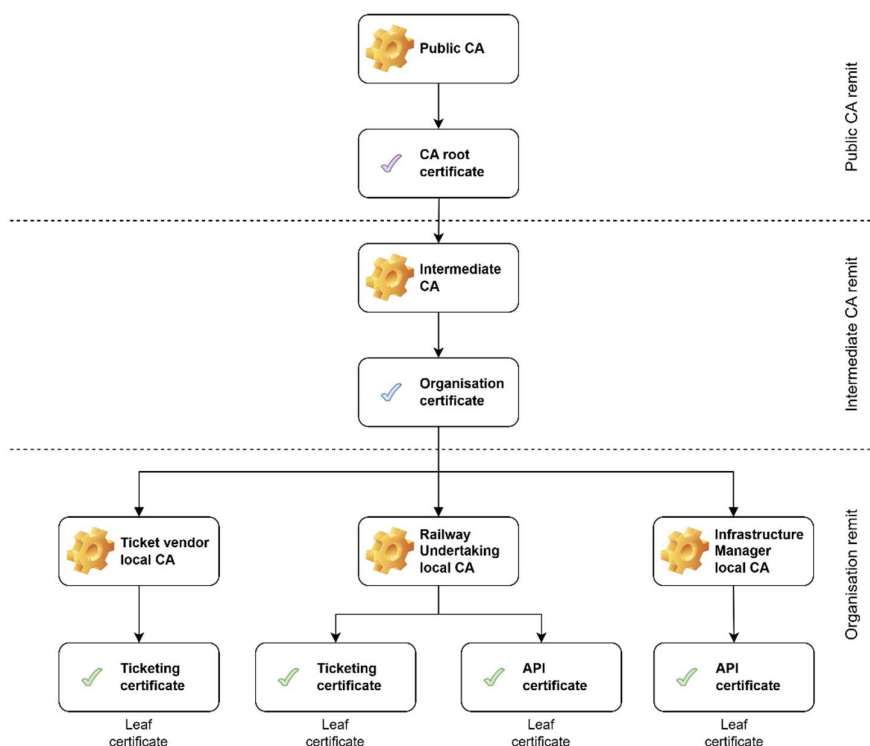


Figure 3 - Overall architecture of the certification chain for telematics PKI

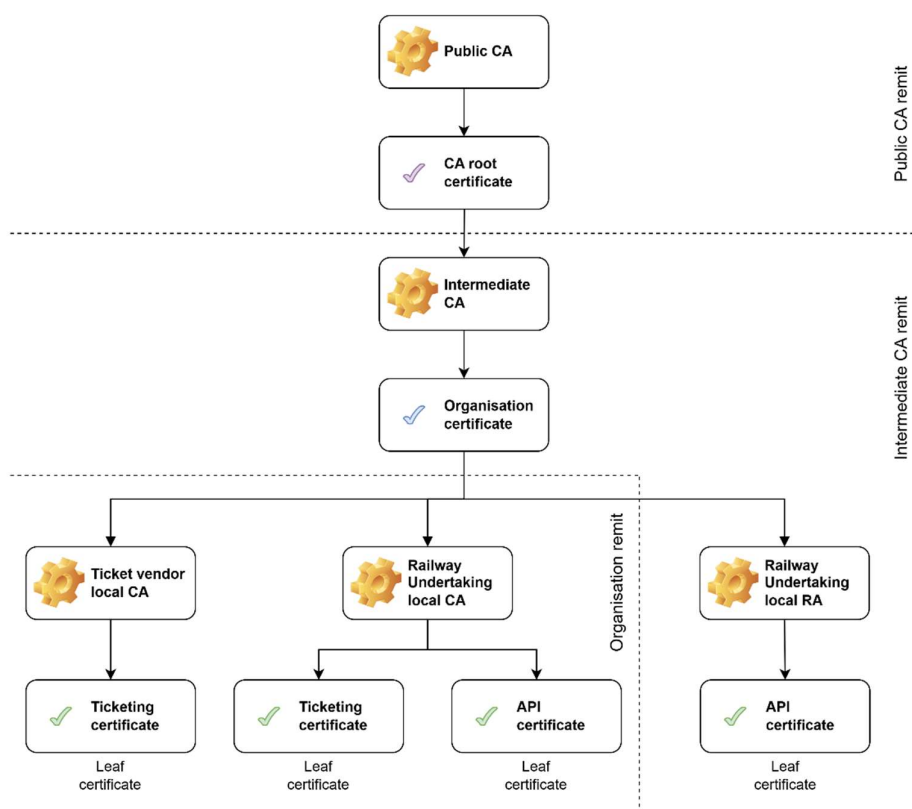


Figure 4 – Hybrid PKI architecture



### 7.1. Organisation certification chain

The certification chain of an organisation (a.k.a. “operator”, as per chart below) is articulated on three levels:

1. The root CA certificate
2. Operational issuing CA certificate
3. The leaf certificates covering communications and human and technical users

The reason for having 1 & 2 is that the root CA provides the foundation of trust, while the issuing CA handles the operational aspects, ensuring security, scalability, flexibility, and efficiency.

The leaf certificates (Table 3) are further specified in the corresponding certificate profiles, describing the parameters for the certificate. The profiles are further explained in 9.1 - Certificate profile.

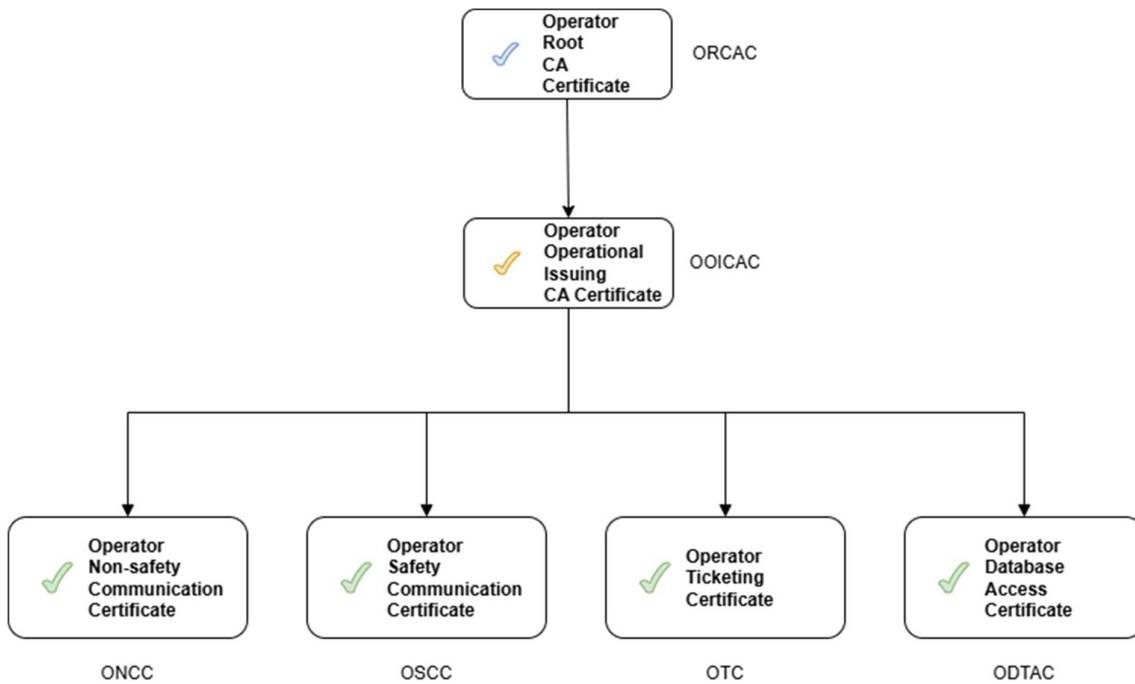


Figure 5 - operator PKI hierarchy for certificates.

Table 3 - types of operator certificates

<i>Certificate Name</i>	<i>Tag</i>	<i>Use Case</i>	<i>Usual Occurrence</i>
Operator Root CA Certificate	ORCAC	ORCAC's are used to certify the identity of an organisation	One to one per organisation
Operator Non-safety Communication Certificate	ONCC	ONCCs are used to protect non safety communication.	zero to multiple ONCCs per actor for RU/IM communication
Operator Safety Communication Certificate	OSCC	OSCCs are used to protect safety communication.	zero to multiple OSCCs per operator
Operator ticketing Certificate	OTC	OTCs are used to secure security elements (e.g. barcodes for ticketing)	zero to multiple OTCs per actor for ticketing purposes
Operator database access certificate	ODTAC	ODTAC are client certificates authorising the access to the addressed database	zero to multiple ODTACs per actor for the access to the reference databases

For the creation of the certificates the following actors must create their certificates for their various use cases of the telematics TSI:

- Railway undertakings
- Infrastructure managers
- Wagon keepers
- Common database providers
- Ticket vendors
- Service providers
- Responsible applicants

Any full certificate chain in the PKI hierarchy of the operator shall contain at least three certificates:

- the CA
- issued organisation certificate,
- the issuing CA certificate of the organisation, and
- the leaf certificate(s).

It is at discretion of the organisation if an internal issuing CA certificate is used.

#### 7.1.1. Certificate requirements

The operator certificate shall fulfil the certificate profile defined in 9.1.1

The Operator Non-Safety Communication Certificate (ONCC) shall fulfil the certificate profile defined in 9.1.2

The Operator Safety Communication Certificate (OSCC) shall fulfil the certificate profile defined in 9.1.3

## 7.2. PKI architecture

The architecture of the PKI shall follow the principles of the certificate management protocol CMP, allowing the automated key exchange and provision. An overall architecture is shown in Figure 6.

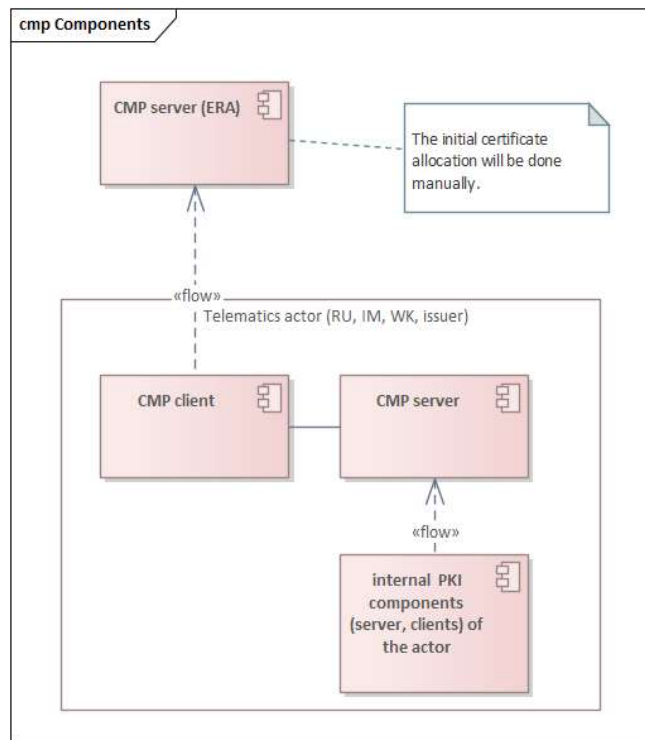


Figure 6 - overall architecture of the PKI

Any CA/RA taking part in the PKI for telematics shall at least support the following messages and their responses of the CMP protocol:

- Initialization Request
- Certification Request
- Key Update Request
- Revocation Request
- Certificate Confirmation

For the RA/CA issuing the organisation certificates, the process shall be managed as manual organisation management process according to 7.6 Initial identity validation. The CA/RA for the organisation certificates ORCAC shall therefor support only the following functions:

- Key Update Request
- Revocation Request
- Certificate Confirmation

#### *7.2.1. Architectural requirements for the organisation certificate ORCAC for RA/CA*

The CA/RA for the requests of the organisation certificates must provide the endpoints according to the requirement SP-SEC-SERV-6.3-10 [10] for key update requests, revocation requests and certificate requests. The provision of the organisation certificates shall be done as a manual process within the Agency. For the re-keying of existing certificates, the requirements according to SP-SEC-SERV-6.3-11 [10] must be supported.

#### *7.2.2. Architectural requirements for other CA/RA*

Each CA/RA must provide the endpoints according to the requirement SP-SEC-SERV-6.3-10 [10] for enrolling of new certificates. For the re-keying of existing certificates, the requirements according to SP-SEC-SERV-6.3-11 [10] must be supported.

### **7.3. Publication and repository responsibilities**

#### *7.3.1. Repositories*

The certificates shall be stored on dedicated repositories at organisational and at functional level (e.g. RU/IM or ticketing). The certificates shall be made publicly available on repositories foreseen for the functional use:

- The Organisation certificates will be stored by the European Union Agency for railways and made publicly available on the website of the Agency.
- Further certificates shall be provided via the certificate management protocol function of the telematics actors.

The certificates shall be published at least 7 days before they become valid.

For ticketing purpose, the certificates shall be published at least 1 month before they become valid.

### **7.4. Identification and authentication**

The identity check has to be done in two cases:

- For the initial identification of the requestor of an organisation certificate
- For the subsequent identification of a requestor in case of a re-keying of an existing certificate

#### *7.4.1. Initial identification*

The requirements for the identity verification are defined in more detail in 7.6 Initial identity validation.

#### *7.4.2. Subsequent identification*

The subsequent identification is based on the proof of identity, provided by the certificate, issued to the entity requesting for the authentication.

## 7.5. Naming

To identify certificates the names used within the certificates must be unique (DN – Distinguished Name). The uniqueness of the organisation certificate will be guaranteed by ERA in their role as RA.

For the naming the usage of the standard X.509 is mandatory.

The following naming components must be used to allow the identification of a unique entity for the certificate:

Table 4 - Naming of certificate attributes

<i>Attribute</i>	<i>Usage</i>
CN	Common Name
OU	Organizational Unit
O	Organization
L	Locality
ST	State or Province Name
C	Country Name
Unique identifier	Organisation code of the entity

## 7.6. Initial identity validation

The identification verification for the organisation certificate follows the two-fold approach of the proposed PKI. The validation of the organisation is part of the registration process of organisations at the registration authority. The issues organisation code is the precondition to issue an organisation certificate (ORCAC). As the Agency serves as RA, the initial identity validation belongs to ERA.

The business specific certificates (e.g. for the RU/IM communication, ticketing) for the operational use of the certificates must be issued by the involved companies in their company specific certification authority process. This process must take into account the organisation certificate, issued by the agency.

### 7.6.1. Identity verification for organisations

For the identification of the organisations the agency is responsible to identify the organisation entity. The identification of the organisations follows the process of the registration of organisations as described in the Commission Implementing Decision (EU) 2018/1614 of 25 October 2018 laying down specifications for the vehicle registers.

Based on this identification an organisation certificate will be issued by the CA and provided via CMP.

### 7.6.2. Identity verification RU/IM, RU/RU, RU/WK communication

The involved railway undertakings and infrastructure managers must agree on their procedures for the initial identity verification of their communication partners. Their certificates must be signed in any case with their organisation certificate, issued by ERA. However additional checks might be necessary to ensure the entity is allowed to take part in the data exchange.

### 7.6.3. Identity verification ticketing

The authentication of the ticketing certificate requests by the issuer must be handled with the railway undertaking, for which the issuer issues tickets. Their certificates must be signed in any case with their organisation certificate, issued by ERA.

The identity of TCO (e.g. railway undertaking or service provider), checking the tickets does not need to be verified.

## 7.7. Identification and authentication for re-key requests

The identification for re-keying requests should follow the key update process as defined in SP-SEC-SERV-6.3-6 of [10].

### **7.8. Identification and authentication for revocation request**

The identification for key revocation requests should follow the key update process as defined in SP-SEC-SERV-6.3-6 of [10].

## 8. Certificate life-cycle operational requirements

### 8.1. Organisation Certificate Application

The following actors are entitled to request a certificate for the various use cases of the telematics TSI:

- Railway undertakings
- Infrastructure managers
- Wagon keepers
- Common database providers
- Ticket issuers (e.g. RU's, ticket vendors)
- Service providers
- Responsible applicants

#### 8.1.1. Organisation certificates

Organisation certificates must be requested by any actors subject to the implementation of Telematics TSI. The process is linked with the process to obtain a new Organization code at the agency<sup>2</sup>.

#### 8.1.2. RU/IM, RU/RU, RU/WK certificates

The certificates shall be managed by the communication partners according to their requirements. The certificates shall be based on the organisation certificate (ORCAC) issued for the parties.

#### 8.1.3. Ticketing certificates

Ticketing certificates must be created by issuers, such as ticket vendors or railway undertakings, to issue tickets according to the Telematics TSI. The certificate shall be created by the ticket issuing undertaking, based on the organisation certificate ORCAC.

### 8.2. Certificate application processing

#### 8.2.1. Organisation certificate (ORCAC) application

The application for the organisation certificate shall follow the rules for the management of the organisation code, as laid down in the Decision (EU) 2018/1614 [5].

#### 8.2.2. Other certificates (ONCC, OSCC, OTAC, PTDAC)

The application for the certificates for the other certificates shall be managed by the issuing entity. All those certificates have to contain the organisation certificate, issued by the agency in tehri certificate chain.

### 8.3. Certificate issuance

The issuance of the organisation certificates (ORCAC) shall be done by the agency. A valid organisation code of the requesting organisation is a precondition for the issuance of a certificate.

### 8.4. Certificate acceptance

Certificates shall be accepted by all actors addressed by the telematics TSI, if the certificate chain includes the organisation certificate, issued and signed by the Agency.

### 8.5. Key pair and certificate usage

The certificates shall be used exclusively for the tasks in scope of this document.

### 8.6. Certificate renewal

The certification renewal is needed to ensure that certificates are valid for a limited time to reduce the risk being compromised and using compromised certificates.

---

<sup>2</sup> [https://www.era.europa.eu/domains/registers/ocr\\_en](https://www.era.europa.eu/domains/registers/ocr_en)

The certification renewal is triggered at least by the maximum lifetime of the certificate. The lifetime of the certificates shall be defined as explained in Table 5 - max lifetime of certificates.

Table 5 - max lifetime of certificates

<i>Certificate type</i>	<i>lifetime</i>
Root	10 years
Organisation certificate	12 months
RU/IM certificate	12 months
RU/RU certificate	12 months
Database access certificate	12 months
Ticketing certificate	12 months recommended, up to 24 months is allowed.

#### 8.6.1. Organisation certificates

The organisation certificates shall be valid for max 12 months. The expiry date of the organisation certificate shall be set to the date when a company ceases operation. If such a date is unknown or not communicated by the company, the certificate expires after 12 months automatically.

#### 8.6.2. RU/IM, RU/RU, database access certificates

The maximum duration of the validity of 12 months must be respected.

#### 8.6.3. Ticketing certificates

Since the signature algorithm DSA is an asymmetric and robust cryptographic procedure, the key pairs must in general be rarely switched. A relative long duration of validity can be chosen.

As general rule, the organisation should choose the shortest duration compatible with the type of ticket. Having said that, the maximum duration of the validity of 12 months should be used. When the ticketing mechanism requires longer duration, it is possible to extend the validity up to 24 months.

Tickets can be valid over longer periods and only one signature per ticket is possible, therefore the validity periods of subsequent keys must overlap. The overlap period must be at least as long as the maximum ticket validity time span (minus 1 day).

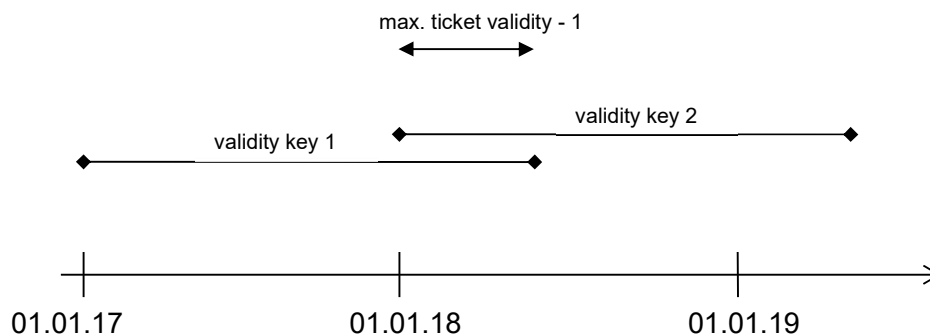


Figure 7 - Example, showing minimum key validity overlap

### 8.6.3.1. Exchange of certificates with partner companies

The period of validity of a key pair is defined as 12 months. Since the certificates must be distributed on the control devices of the different RUs, the exchange of a certificate must take place in advance of its validity time span.

## 8.7. Certificate re-key

Certificate re-keying shall take place at least when the validity period of the certificate has been reached. More frequent re-keying is possible, if needed. Re keying

## 8.8. Certificate modification

Certification modifications, such as the change of certificate names or components, is not permitted. If changes of the certificates are necessary, a certificate renewal request with the changed new data must be submitted to the involved RA/CA.

## 8.9. Certificate revocation and suspension

Organization certificates (ORCAC) shall be revoked by the Agency for justified reasons, such as:

- **Compromise of Private Key:** If the private key associated with a certificate is compromised (e.g., stolen or hacked), the certificate must be revoked to prevent unauthorized use.
- **Change in Affiliation:** If an employee leaves an organization or a device is no longer used, the certificates issued to them should be revoked to ensure they can no longer access secure resources.
- **Certificate Misuse:** If a certificate is found to be used inappropriately or fraudulently, it will be revoked to stop the misuse.
- **Security Vulnerability:** If a vulnerability is discovered in the cryptographic algorithms or protocols used by the certificate, it may be revoked to protect against potential attacks.
- **Expiration:** Sometimes certificates are revoked before their expiration date if they are no longer needed or if they were issued incorrectly.
- **Policy Violations:** If the certificate holder violates the terms of use or policies set by the Certificate Authority (CA), the certificate can be revoked.

When a certificate is revoked, it is added to a Certificate Revocation List (CRL) or its status is updated via the Online Certificate Status Protocol (OCSP), allowing systems to check and ensure the certificate is no longer trusted.

## 8.10. Certificate status services

All CMP servers have to support a certificate status service.

# 9. Certificate, CRL and OCSP profiles

## 9.1. Certificate profile

### 9.1.1. Operator profile

The content of the operator certificate (OOICAC) is defined in the table below.

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	Elliptic Curve Cryptography	
Issuer	[Subject DN of OOICAC of the operator]	
Validity	[organisation-specific validity period]	



Subject mandatory:	mandatory: CN=[unique operator-specific CN] recommended: OU=[operator-specific organization] C=[operator-specific country]	Additional issuer-specific attributes are allowed
Subject Public Key Info	[public key]	
X.509 v3 Extensions		
Authority Key Identifier	[key identifier of issuer public key]	
Subject Key Identifier	[key identifier of own public key]	
Key Usage (critical)	digitalSignature	
Subject Alternative Name	[operator-specific]	optional
Certificate Policies	[operator-defined policy information]	optional
CRL	Link to CRL	

### 9.1.2. Operator Non-Safety Communication (ONCC) profile

See SP-SEC-SERV-13.1.2-2 in [8].

### 9.1.3. Operator Safety Communication (OSCC) profile

See SP-SEC-SERV-13.1.2-3 in [8].

### 9.1.4. Operator ticketing Certificate

The content of the ticketing certificate is defined in the table below.

<i>Field Name</i>	<i>Content</i>	<i>Comment</i>
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	dsa_with_SHA256	legacy implementation, otherwise ECC
Issuer	[Subject DN of OOICAC of the operator]	
Validity	[ticket issuer-specific period]	recommended validity period is 1 year, when needed the validity can be extended to 24 months
Subject mandatory:	mandatory: CN=[unique operator-specific CN] recommended: OU=[operator-specific organization] C=[operator-specific country]	Additional issuer-specific attributes are allowed
Subject Public Key Info	[public key]	
X.509 v3 Extensions		
Authority Key Identifier	[key identifier of issuer public key]	
Subject Key Identifier	[key identifier of own public key]	
Key Usage (critical)	digitalSignature	
Subject Alternative Name	[operator-specific]	optional
Certificate Policies	[operator-defined policy information]	optional
CRL	Link to the CRL	

**9.2. CRL profile**

<i>Field Name</i>	<i>Content</i>	<i>Comment</i>
Version	0x2	X.509 v3
Signature Algorithm	dsa_with_SHA256	
Issuer	[Subject DN of ORCAC of the operator]	
Validity	[organisation-specific validity period]	
Subject mandatory:	mandatory: CN=[unique operator-specific CN] recommended: OU=[operator-specific organization] C=[operator-specific country]	
Effective Date		
Next Update		
Revoked Certificates	List of revoked certificates.	
Serial Number	[integer]	
Revocation Date	Date and time of revocation of the certificate	
Reason code	Reason code for certificate revocation.	1 – (keyCompromise); 2 – (cACompromise); 3 – (affiliationChanged); 4 – (superseded); 5 – (cessationOfOperation).
Signature	[operator-specific]	optional

## **Annex I – Organisational requirements for a Certification Authority**

### **Preconditions**

The organisation will have to have an Information Security Management System in line with the standard ISO 27001.

The root certificate will have to be signed by a Qualified Trust Service Provider under the EU Regulation No. 910/2014.

Additional specific provisions are the following:

## 1. Context of the Organization

### 1.1. Understanding the Organization and Its Context

- 1.1.1. *Identify stakeholders and understand the regulatory, operational, and technical environments.*
- 1.1.2. *Define services including certificate issuance for railway systems.*

### 1.2. Understanding the Needs and Expectations of Interested Parties

- 1.2.1. *Document legal, regulatory, and contractual obligations.*
- 1.2.2. *Address sector-specific requirements.*

### 1.3. Determining the Scope of the CA's Trust Services

- 1.3.1. *Define scope in CP/CPS including certificate types and assurance levels.*

## 2. Leadership

### 2.1. Leadership and Commitment

- 2.1.1. *Ensure senior management commitment and alignment with applicable ETSI, ISO, EC standards.*

### 2.2. Policy

- 2.2.1. *Define an information security and trust service policy.*

### 2.3. Roles, Responsibilities, and Authorities

- 2.3.1. *Define roles, ensure role segregation, and maintain job descriptions.*

## 3. Planning

### 3.1. Actions to Address Risks and Opportunities

- 3.1.1. *Conduct risk assessments and establish response procedures.*

### 3.2. Objectives and Planning to Achieve Them

- 3.2.1. *Define measurable objectives and KPIs.*

### 3.3. Planning for Change

- 3.3.1. *Apply change management and inform stakeholders.*

## 4. Support

### 4.1. Resources

- 4.1.1. *Ensure adequate resources (e.g., staff, infrastructure).*

### 4.2. Competence

- 4.2.1. *Hire, train, and evaluate qualified personnel.*

### 4.3. Awareness

- 4.3.1. *Ensure staff understand policies and responsibilities.*

### 4.4. Communication

- 4.4.1. *Maintain clear internal and external communication channels.*

### 4.5. Documented Information

4.5.1. *Maintain and control all operational and compliance documents.*

## **5. Operations**

### **5.1. Operational Planning and Control**

5.1.1. *Manage certificate lifecycle and secure cryptographic operations.*

### **5.2. Outsourced Processes**

5.2.1. *Control third-party providers through SLAs and audits.*

### **5.3. Change Management**

5.3.1. *Authorize and document operational changes.*

### **5.4. Security Controls Implementation**

5.4.1. *Enforce physical, logical, and system security measures.*

## **6. Performance Evaluation**

### **6.1. Monitoring, Measurement, Analysis, and Evaluation**

6.1.1. *Monitor KPIs, maintain logs, and evaluate security events.*

### **6.2. Internal Audit**

6.2.1. *Conduct regular audits of CA operations and compliance.*

### **6.3. Management Review**

6.3.1. *Review audit results, incidents, and performance indicators.*

## **7. Improvement**

### **7.1. Risks and mitigating measures**

7.1.1. *Document the contribution of risk assessment to the overall CA performance improvement*

### **7.2. Nonconformity and Corrective Action**

7.2.1. *Document and resolve non-conformities with root cause analysis.*

### **7.3. Continual Improvement**

7.3.1. *Use feedback and assessments to improve trust services.*

## Annex II – Technical requirements

### 1. For Certification/Registration authorities


Source: Technical Interface Specifications – Cybersecurity “SP-SEC-ServSpec” [10]





Europe's Rail System Pillar Publication  
Technical Interface Specification - Cybersecurity  
SP-SEC-ServSpec - V1.0 - February 2025


[REDACTED]


#### 6.3 PKI CA/RA requirements


 **SP-SEC-Serv-6.3-1** - The PKI CA mentioned in this chapter is the CA installed in the operators environment, not the manufacturer CA.


 **SP-SEC-Serv-6.3-2** - The SSI-PKI shall issue X.509 v3 certificates as defined in [SP-SEC-Serv-2.3-9](#) - [RFC 5280].


 **SP-SEC-Serv-6.3-3** - The SSI-PKI shall issue certificates according to the certificate profiles defined in [14.1 - Certificate Profiles](#).

 **SP-SEC-Serv-6.3-4** - The PKI RA/CA shall provide the capability to issue, rekey, and revoke certificates using the CMP protocol via HTTP according to the Lightweight CMP Profile (LCMPP) as defined in [SP-SEC-Serv-2.3-24](#) - [RFC 9483].


 **SP-SEC-Serv-6.3-5** - The PKI RA/CA shall support the following CMP messages: Initialization Request (ir), Certification Request (cr), Key Update Request (kur), Revocation Request (rr), Certificate Confirmation (certConf) and their associated responses (ip, cp, kup, rp, pkiConf, error).

 **SP-SEC-Serv-6.3-6** - The PKI RA/CA shall validate the content and signature-based message protection of every received CMP request according to Section 3.5 in [SP-SEC-Serv-2.3-24](#) - [RFC 9483] before accepting it.


 **SP-SEC-Serv-6.3-7** - The PKI RA/CA shall handle errors according to Section 3.6.2 of [SP-SEC-Serv-2.3-24](#) - [RFC 9483].

 **SP-SEC-Serv-6.3-8** - The PKI RA/CA shall provide CRLs compliant to [SP-SEC-Serv-2.3-9](#) - [RFC 5280] via HTTP.

Note: Secure CRL download via HTTPS is not necessary, because CRLs are signed by the respective CA.

 **SP-SEC-Serv-6.3-9** - CRLs provided by the PKI RA/CA shall contain the nextUpdate field.

Note: recommended update period is 24h.

 **SP-SEC-Serv-6.3-10** - The PKI RA/CA shall send a pkiConf message at the reception of the certConf message.

Note: this means that ImplicitConfirm is not used.


 **SP-SEC-Serv-6.3-11** - The PKI RA/CA shall provide the following CMP endpoints according to Section 6.1 of [SP-SEC-Serv-2.3-24](#) - [RFC 9483] for enrolling new certificates matching the certificate profiles chapter 6.3.2.



Table 4 CMP endpoints for enrolling new certificates

CMP Endpoint URL	Issued Certificate Types	Endpoint Protection
<code>/ .well-known/cmp/p/ODC/initialization</code>	ODC	CMP requests: message protection with MDC CMP responses: message protection with issuing CA key
<code>/ .well-known/cmp/p/ONCC/certification</code>	ONCC	CMP message protection with ODC CMP responses: message protection with issuing CA key
<code>/ .well-known/cmp/p/OSCC/certification</code>	OSCC	CMP message protection with ODC CMP responses: message protection with issuing CA key

☑, **SP-SEC-Serv-6.3-12** - The PKI RA/CA shall provide the following CMP endpoints according to Section 6.1 of **SP-SEC-Serv-2.3-24 - [RFC 9483]** for rekeying existing certificates via Key Update Request (kup).

Table 5 CMP endpoints for rekeying existing certificates

CMP Endpoint URL	Issued Certificate Types	Endpoint Protection
<code>/ .well-known/cmp/p/ODC/keyupdate</code>	ODC	CMP requests: message protection with ODC CMP responses: message protection with issuing CA key
<code>/ .well-known/cmp/p/ONCC/keyupdate</code>	ONCC	CMP message protection with ONCC CMP responses: message protection with issuing CA key
<code>/ .well-known/cmp/p/OSCC/keyupdate</code>	OSCC	CMP message protection with OSCC CMP responses: message protection with issuing CA key

☑, **SP-SEC-Serv-6.3-13** - The PKI RA shall use an Operator Non-Safety Communication Certificate (ONCC) to sign the following CMP messages sent from RA to CA according to Section 5.2.2.1 of **SP-SEC-Serv-2.3-24 - [RFC 9483]**: Initialization Request (ir), Certification Request (cr), and Revocation Request (rr).

☑, **SP-SEC-Serv-6.3-14** - The PKI RA shall only forward correctly authenticated and authorized CMP requests (see **SP-SEC-Serv-2.3-24 - [RFC 9483]** Sections 3.5, 5.1.1 and 5.1.2) to the PKI CA (see Tables **SP-SEC-Serv-6.3-11** and **SP-SEC-Serv-6.3-12**).

☑, **SP-SEC-Serv-6.3-15** - The PKI CA shall only accept CMP requests if they are correctly signed by the RA's ONCC see **SP-SEC-Serv-2.3-24 - [RFC 9483]** Sections 3.5, 5.1.1 and 5.1.2).

Note: the RA's ONCC can be identified by matching its unique CN to a preconfigured value.

☑, **SP-SEC-Serv-6.3-16** - The PKI RA/CA shall support the following protection algorithms for creating signatures to protect its CMP responses: ecdsa-with-SHA256, ecdsa-with-SHA384, ecdsa-with-SHA512 according to Section 3.2 of **SP-SEC-Serv-2.3-23 - [RFC 9481]**.

Note: **SP-SEC-Serv-6.3-11** and **SP-SEC-Serv-6.3-12** define which key to use for every CMP endpoint.



## 2. For PKI clients



Europe's Rail System Pillar Publication  
Technical Interface Specification - Cybersecurity  
SP-SEC-ServSpec - V1.0 - February 2025

### 6.4 PKI client requirements

☑, **SP-SEC-Serv-6.4-1** - The SSI-PKI client shall provide the capability to request and rekey certificates using the CMP protocol via HTTP according to the Lightweight CMP Profile (LCMP) [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#).

Note: Confidentiality protection is not needed because only public data is transferred. Since CMP includes integrity protection, an insecure transport protocol (HTTP in this case) can be used.

☑, **SP-SEC-Serv-6.4-2** - When requesting certificates, the SSI-PKI client shall sign the CMP Initialization Request message (ir) and certConf with MDC ([SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) Section 4.1.1) and the CMP Certification Request message (cr) and certConf with ODC ([SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) Section 4.1.2) according to [SP-SEC-Serv-6.3-11](#).

☑, **SP-SEC-Serv-6.4-3** - When rekeying a certificate, the SSI-PKI client shall use the private key associated with the certificate to sign the CMP Key Update Request message (kup) and certConf (see [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) Section 4.1.3).

☑, **SP-SEC-Serv-6.4-4** - When revoking a certificate, the SSI-PKI client shall use the private key associated with the certificate to sign the CMP Revocation Request (rr) (see [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) Section 4.2).

☑, **SP-SEC-Serv-6.4-5** - The SSI-PKI client shall sign CMP requests by using ecdsa-with-sha256 as protectionAlg as defined in Section 3.2 of [SP-SEC-Serv-2.3-23 - \[RFC 9481\]](#).

☑, **SP-SEC-Serv-6.4-6** - The SSI-PKI client shall support the following CMP messages: Initialization request (ir), Certification Request (cr), Key Update Request (kur), Certificate Confirmation (certConf) and their associated responses (ip, cp, kup, pkiConf, error) as defined in [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#).

☑, **SP-SEC-Serv-6.4-7** - The SSI-PKI client shall validate the content and signature-based message protection of every received CMP message according to [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) section 3.5 before accepting it.

Note: Any error condition should be handled according to [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) Section 3.6.1.

☑, **SP-SEC-Serv-6.4-8** - The SSI-PKI client shall request and rekey certificates needed for operation.

☑, **SP-SEC-Serv-6.4-9** - The SSI-PKI client shall download CRLs via HTTP and process CRLs as defined in [SP-SEC-Serv-2.3-9 - \[RFC 5280\]](#) using a URL defined in the CRL Distribution Point (CDP) extension, which can be overwritten by a URL defined in the client's configuration.

☑, **SP-SEC-Serv-6.4-10** - The PKI client shall send a certConf message at the reception of the ip, cp, or kup message according to [SP-SEC-Serv-2.3-24 - \[RFC 9483\]](#) Section 4.1.1.

☑, **SP-SEC-Serv-6.4-11** - The PKI client shall support the following protection algorithms for creating signatures to protect its CMP requests: ecdsa-with-SHA256, ecdsa-with-SHA384, ecdsa-with-SHA512 according to Section 3.2 of [SP-SEC-Serv-2.3-23 - \[RFC 9481\]](#).

Note: [SP-SEC-Serv-6.3-11](#) and [SP-SEC-Serv-6.3-12](#) define which key to use for every CMP endpoint.