Disclaimer

This document is

the final draft created in September 2024 for the third and final review period (September 23rd - October 31st 2024) before planned publication in January 2025.

Please consider the semantics of the following **work item types** used in this document when preparing your review.

drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

EU Rail authorizes you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following mention [EU Rail trade mark, title of the document, year of publication, version of document, URL].

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models inthis document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trademarks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address:

cybersecurity.review@ertms.be

Work Item Type	Icon	Rationale
System Requirement	☞	Used for mandatory requirements.
Text	📄	Used for prose text, e.g. as an introduction or for additional information. The contents of these work items are **not requirements.**
Issue	☰	Used for open issues to be addressed in the final version. The contents of these work items are **not requirements.**

First draft version (01/2024) includes:

- import of EULYNX BL4 R2 and UNISIG Subset 146 content
- review requirements

Second draft version (02/2024) includes

- generally reworked structure of the document
- updated according to review comments from 1st draft review

Final draft (V0.90 03/2024) includes

- updated according to review comments from 2nd draft review
- new specification text to close the open issues

11 BKP: Backup and Restore

12 Security Requirements for DNS

13 Annex

13.1 Certificate Profiles

13.1.1 Manufacturer Certificate Profiles

13.1.2 Operator Certificate Profiles

, SP-SEC-SERVServ-32.1-1 - This specification defines the standard security interfaces (SSI) to the Shared Cybersecurity Services : SSI-STS, SSI-PKI, SSI-IAM, SSI-NAC, SSI-LOG, SSI-UAS, SSI-BKP, SSI-DNS.

Note(SCS) and proposes the interfaces from SCS to the Enterprise Security Services (ESS) for the following services: STS, PKI, IAM, NAC, LOG, UAS, BKP, DNS.

Note1: "interface" in the context of this specification is used as a network-based interface **[**SPPRAMSS-1498 **]**

Note2: for an explaination of these abbreviations, see Table 1

Note3: IAM does not cover human user authorization, for this, UAS is used

, SP-SEC-SERVServ-32.1-2 - A Shared Cybersecurity Service provides common security functions used by other Secure Components. **[**SPPRAMSS-8220 **]**

, SP-SEC-SERVServ-32.1-3 - The Shared Cyber Security Cybersecurity Services are used via the interfaces described in this document by Secure Components and are required for interoperability in and harmonisation of the European rail automation domain. **[**SPPRAMSS-1497 **]**

, SP-SEC-SERVServ-32.1-4 - The interfaces described in this document are specified so that temporal unavailability (e.g. a few hours to days) has no direct impact on rail operation. **[**SPPRAMSS-7176 **]**

, SP-SEC-SERVServ-32.1-5 - For the a definition of key termterms, see 10 Taxonomy and References. **[**SPPRAMSS-10317 **]**

, SP-SEC-Serv-2.2-1 - This specification uses identifiers starting with "SP-SEC-Serv".

, SP-SEC-Serv-2.2-2 - Icon types used in this document are defined in SP-SEC-Tax.

, SP-SEC-Serv-2.3-1 - This chapter contains all references of this document. For a complete list including external references see SP-SEC-Tax Chapter 2

[IANA PENs]

Private Enterprise Numbers (PENs)

[IANA SMI PKIX EKU]

SMI Security for PKIX Extended Key Purpose

[OIDC 1.0]

OpenID Connect Core 1.0

[IEEE 802.1X-2020]

IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control

[RFC 1952]

GZIP file format specification version 4.3

[RFC 2865]

Remote Authentication Dial In User Service (RADIUS)

[RFC 4086]

Randomness Requirements for Security

[RFC 5280]

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC 5424]

The Syslog Protocol

[RFC 5425]

Transport Layer Security (TLS) Transport Mapping for Syslog

[RFC 5905]

Network Time Protocol Version 4: Protocol and Algorithms Specification

[RFC 7636]

Proof Key for Code Exchange by OAuth Public Clients

[RFC 7643]

System for Cross-domain Identity Management: Core Schema

[RFC 7644]

System for Cross-domain Identity Management: Protocol

[RFC 7858]

Specification for DNS over Transport Layer Security (TLS)

[RFC 8176]

Authentication Method Reference Values

[RFC 8446]

The Transport Layer Security (TLS) Protocol Version 1.3.

[RFC 8915]

Network Time Security for the Network Time Protocol

[RFC 9150]

TLS 1.3 Authentication and Integrity-Only Cipher Suites

[RFC 9190]

EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3

[RFC 9364]

DNS Security Extensions (DNSSEC)

[RFC 9481]

Certificate Management Protocol (CMP) Algorithms

[RFC 9483]

Lightweight Certificate Management Protocol (CMP) Profile

[RFC 9662]

Updates to the Cipher Suites in Secure Syslog

[RFC automation-keyusages]

X.509 Certificate Extended Key Usage (EKU) for Automation

Note: this RFC is a draft, the actual RFC number will be added in a future version of this document

[SP-SEC-CompSpec]

Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.0

[SP-SEC-CommSpec]

Europe's Rail System Pillar Cybersecurity Domain - Secure Commmunication Specification, v1.0

Secure Component

An implementation, as part of an automation control system, either a host device, embedded device, network device or software application on a host device, which realizes subsystem functions, implements security capabilities and consisting of a physical encasing, computing capabilities and network communication, and interfacing to the Shared Cybersecurity Services.

Examples of CCS secure components are object controller, trackside cabinet, IXL rack, ATO-OB, OBU, ATO-TS, IXL/RBC combination, shared cybersecurity services, security proxy for legacy devices, …)

Examples of components which are not meeting the definition of a Secure Component are components with no network communication, e.g. directly connected sensors or displays.

Shared Cybersecurity Services (SCS)

A collection of standard security interfaces (SSIs) of central security functions accessible for all Secure Components in the automation solution. The realization of the Shared Cybersecurity Services (SCS) implements the requirements of the Secure Component Specification as they are considered as Secure Components as well.

The interfaces from Secure Components to Shared Cybersecurity Service are identified by SSI-<service name>.

The Shared Cybersecurity Services implementations are identified by SCS-<service name>.

Enterprise Cybersecurity Services

A collection of enterprise security interface (ESI) implementations of central security and IT communication functions in a back-office environment.

Examples are Security Incident and Event Management System (SIEM), Intrusion Detection System, PKI Certificate Authority, Corporate Directory, Asset Management, DNS. These services are typically accessible for the automation network via controlled communication paths (e.g. DMZ). The interfaces of the Shared Cybersecurity Services to the Enterprise Services are identified by ESI-<Service name>.

Note: Enterprise Shared Services are typically 3rd-party components not dedicated to the rail environment. Therefore the realization of the Enterprise Shared Services may use other security requirements than the Secure Component Specification. Recommended security specification are ISO 27033,

ISO 27034, NIST 800-53, and/or IEC 62443-4-2.
Note: Enterprise Shared Services and Shared Cybersecurity Services are separated by the IT/OT border (e.g. by a DMZ).

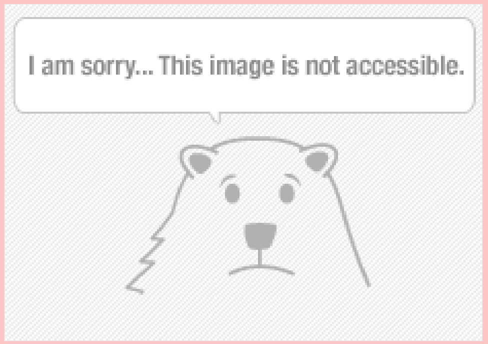
First release (V1.0) - February 2025

- reviewed by System Pillar domains, rail cybersecurity mirror groups, external organizations in three review rounds during 2024

, **SP-SEC-SERVServ-3.2-1 -** This scheme shows an exemplary hierarchy and interfaces (arrows) of shared services between each other, as well the association to external services. The Figure figure includes:

- the Shared Cybersecurity Services (SCS) which offer mandatory Standard Security Interfaces (SSI) to Secure Components
- the Enterprise Cybersecurity Services (ECS), which offer recommended Enterprise Security Interfaces (ESI) to SCS
- external services on a national level used by the ECS

SSI are for the OT (operational technology) environment, the ESI are between the OT and IT environment, therefore crossing a trust boundary. SimilarySimilarly, interfaces between ECS and national services also cross a trust boundary from IT environment to Internet services.



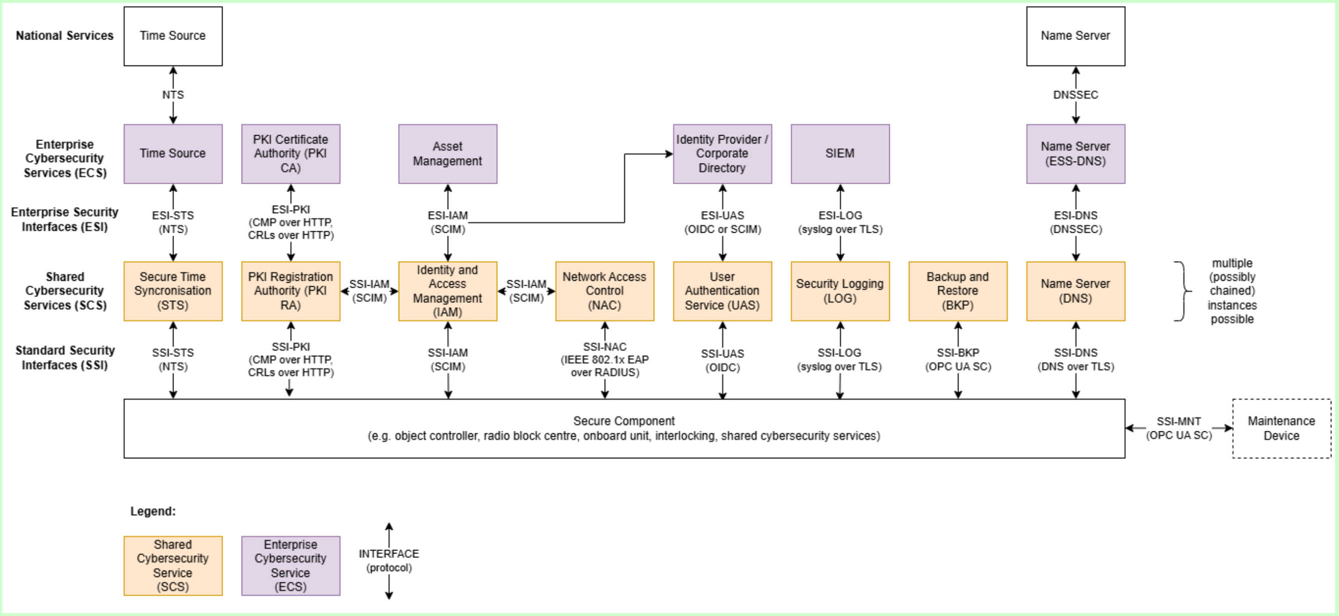

National Services
Time Source
NTS
Name Server
DNSSEC
Enterprise Cybersecurity Services (ECS)
Time Source
PKI Certificate Authority (PKI CA)
Asset Management
Identity Provider / Corporate Directory
SIEM
Name Server (ESS-DNS)
Enterprise Security Interfaces (ESI)
ESI-STS (NTS)
ESI-PKI (CMP over HTTP, CRLs over HTTP)
ESI-IAM (SCIM)
ESI-UAS (OIDC or SCIM)
ESI-LOG (syslog over TLS)
ESI-DNS (DNSSEC)
Shared Cybersecurity Services (SCS)
Secure Time Syncronisation (STS)
PKI Registration Authority (PKI RA)
SSI-IAM (SCIM)
Identity and Access Management (IAM)
SSI-IAM (SCIM)
Network Access Control (NAC)
User Authentication Service (UAS)
Security Logging (LOG)
Backup and Restore (BKP)
Name Server (DNS)
multiple (possibly chained) instances possible
Standard Security Interfaces (SSI)
SSI-STS (NTS)
SSI-PKI (CMP over HTTP, CRLs over HTTP)
SSI-IAM (SCIM)
SSI-NAC (IEEE 802.1x EAP over RADIUS)
SSI-UAS (OIDC)
SSI-LOG (syslog over TLS)
SSI-BKP (OPC UA SC)
SSI-DNS (DNS over TLS)
Secure Component
(e.g. object controller, radio block centre, onboard unit, interlocking, shared cybersecurity services)
SSI-MNT (OPC UA SC)
Maintenance Device
Legend:
Shared Cybersecurity Service (SCS)
Enterprise Cybersecurity Service (ECS)
INTERFACE (protocol)

Figure 1 Overview of the Shared Cybersecurity Services and their Interfaces

[SPPRAMSS-4670]

Note: This is a schematic view, a real-world implementation incorporates a more complex federated structure (e.g. multiple deployments of the same services in different domains such as rail automation, electrification, stations, freight, ...). Additionally, a more complex hierarchy involving multiple levels (e.g. onboard / trackside deployments) is possible.

, SP-SEC-SERVServ-3.2-2 - The following table gives an overview of the security services described in this document:. While for the SSI, the use of specific protocols is required, this document only gives recommendations for protocols to use in ESI.

Table 1 Overview of Shared Cybersecurity Services

Chapter - Shared Cybersecurity Service	**Interface(s)**
	SSI = Shared Cybersecurity standard security interface
	ESI = enterprise security interface
		Mandatory	**Description**

5 - STS: Secure Time Synchronisation	SSI-STS ESI-STS	yes	service for secure time synchronisation to Secure Components, particularly important to validate certificates
6 - PKI: Public Key Infrastructure	SSI-PKI ESI-PKI	yes	service for distributing certificates and their revocation status to Secure Components, crucial for all secure communication
7 - IAM: Identity and Access Management	SSI-IAM ESI-IAM	yes	service for managing digital identities (of components and users) **Comment:** The SSI-IAM interface is only used for machine-to-machine communication). Humans use the SSI-UAS interface.
8 - NAC: Network Access Control	SSI-NAC	yes	service for identifying, authenticating, and authorizing network access of Secure Components
9 - LOG: Security Logging	SSI-LOG ESI-LOG	yes	service for collecting log messages from Secure Components and relaying log messages (e.g. to another relay or SIEM)
10 - UAS: User Authentication Service	SSI-UAS ESI-UAS	for human users	service for managing roles for authorisation and user authentication **Comment:** SSI-UAS is only needed when human user access is required (i.e. not needed for machine-to-machine communication which is based on SSI-PKIcertificates)
11 - BKP: Backup and Restore	SSI-BKP	for devices with state	service for creating and restoring backups to/from Secure Components **Comment:** SSI-BKP is not needed when there is nothing to back up (e.g. on devices without state with fixed configuration)

Chapter - Shared Cybersecurity Service	Interface(s)
	SSI = Shared Cybersecurity standard security interface
	ESI = enterprise security interface
		Mandatory	Description

12 - MNT: Security Maintenance	SSI-MNT	yes	interface for security-related maintenance functions
1213 - Security Requirements for DNS	SSI-DNS ESI-DNS	only when DNS is used	service for name resolution to map domain names to IP addresses. **Comment**: SSI-DNS is not needed when DNS is not used

[SPPRAMSS-5254]

, SP-SEC-SERVServ-3.2-3 - For most Shared Cybersecurity Services, an onboard deployment with a caching functionality is recommended. These onboard Cybersecurity Services provide interfaces using data synchronised from wayside Shared Cybersecurity Services when wayside network connection is not available:

- **STS** - Secure Time Synchronisation
- **NAC** - Network Access Control
- **DNS** - Domain Name System
- **IAM** - Identity and Access Management
- **UAS** - User Authentication Service
- **LOG** - Security Logging

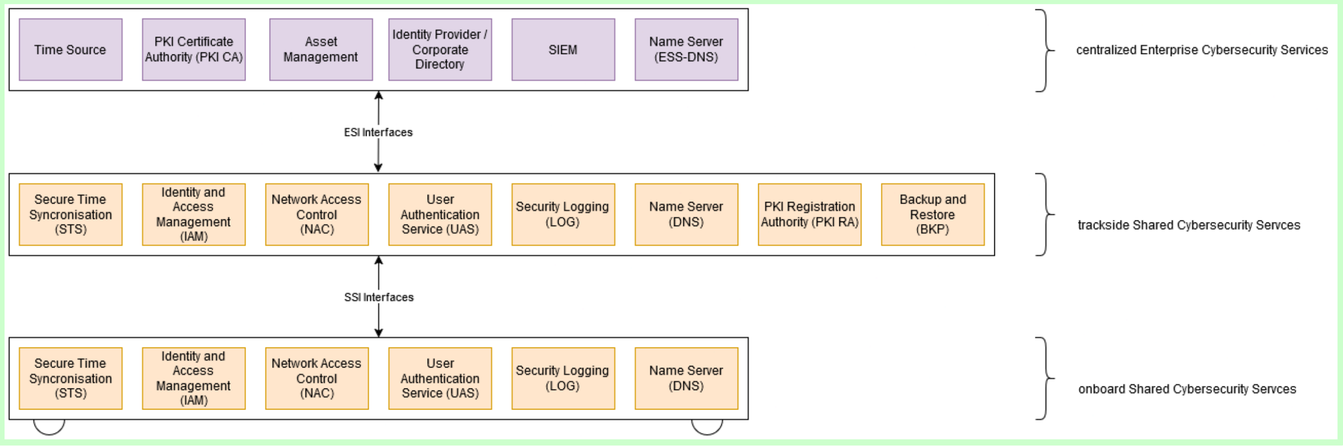
The following Services are by default not needed for daily operation and therefore do not need impose an onboard deployment:

- **PKI RA** - Public Key Infrastructure Registration Authority
- **BKP** - Backup and Restore

[SPPRAMSS-9699]

-

  The following figure shows the an example onboard/trackside deployment.


Time Source
PKI Certificate Authority (PKI CA)
Asset Management
Identity Provider / Corporate Directory
SIEM
Name Server (ESS-DNS)
centralized Enterprise Cybersecurity Services
ESI Interfaces
Secure Time Syncronisation (STS)
Identity and Access Management (IAM)
Network Access Control (NAC)
User Authentication Service (UAS)
Security Logging (LOG)
Name Server (DNS)
PKI Registration Authority (PKI RA)
Backup and Restore (BKP)
trackside Shared Cybersecurity Servces
SSI Interfaces
Secure Time Syncronisation (STS)
Identity and Access Management (IAM)
Network Access Control (NAC)
User Authentication Service (UAS)
Security Logging (LOG)
Name Server (DNS)
onboard Shared Cybersecurity Servces

, SP-SEC-SERV-3.3-1 - references will be added later

references will be added later **[**SPPRAMSS-6753 **]**

, SP-SEC-SERV-3.4-1 - acronyms and abbreviations will be added later

acronyms and abbreviations will be added later **[**SPPRAMSS-6752 **]**

, SP-SEC-SERV-3.5-1 - terms and defintions will be added later

[SPPRAMSS-6754 **]**

, SP-SEC-SERVServ-4-1 - All implementations of Shared Cybersecurity Services shall fullfill the requirements of the Secure Component Specification.SP-SEC-Serv-2.3-27 - [SP-SEC-CompSpec].
Note: Implementations of the Enterprise Security Services are assumed to be built according to comparable standards, e.g. ISO 27k. **[**SPPRAMSS-3692 **]**

, SP-SEC-SERV-4-2 - All instances of Shared Cybersecurity Services shall be addressed via IP address and/or FQDN. Reference to Network Essential Requirements document: Essential Network Requirements **[**SPPRAMSS-8040 **]**

, SP-SEC-SERVServ-4-32 - The SSI interfaces do not require any network priorization. All interfaces prioritization over voice or safety communication. There is no distinction of service prioritization among the SSI. All SSI can use best effort QoS class. **[**SPPRAMSS-10041 **]**

, SP-SEC-Serv-4-3 - The Standard Security Interfaces (SSI) shall use the protocols listed in the following table:

Interface SSI = standard security interface	**Protocols**	**References**
SSI-STS	NTS	SP-SEC-Serv-2.3-19 - [RFC 8915]
SSI-PKI	CMP over HTTP, CRLs over HTTP	SP-SEC-Serv-2.3-9 - [RFC 5280] SP-SEC-Serv-2.3-24 - [RFC 9483]
SSI-IAM	SCIM 2.0	SP-SEC-Serv-2.3-14 - [RFC 7643] SP-SEC-Serv-2.3-15 - [RFC 7644]

Interface SSI = standard security interface	**Protocols**	**References**
SSI-NAC	IEEE 802.1x EAP over RADIUS	SP-SEC-Serv-2.3-5 - [IEEE 802.1X-2020] SP-SEC-Serv-2.3-21 - [RFC 9190] SP-SEC-Serv-2.3-7 - [RFC 2865]
SSI-UAS	OIDC	SP-SEC-Serv-2.3-4 - [OIDC 1.0]
SSI-LOG	syslog over TLS	SP-SEC-Serv-2.3-11 - [RFC 5425] SP-SEC-Serv-2.3-25 - [RFC 9662]
SSI-DNS	DNS over TLS	SP-SEC-Serv-2.3-16 - [RFC 7858]

, SP-SEC-Serv-4-4 - The recommended protocols for the Enterprise Security Interfaces (ESI) are listed in the following table:

Interface ESI = enterprise security interface	**Protocols**	**References**
ESI-STS	NTS	SP-SEC-Serv-2.3-19 - [RFC 8915]
ESI-PKI	CMP over HTTP, CRLs over HTTP	SP-SEC-Serv-2.3-9 - [RFC 5280] SP-SEC-Serv-2.3-24 - [RFC 9483]
ESI-IAM	SCIM 2.0	SP-SEC-Serv-2.3-15 - [RFC 7644]
ESI-UAS	OIDC or SCIM 2.0	SP-SEC-Serv-2.3-4 - [OIDC 1.0] SP-SEC-Serv-2.3-15 - [RFC 7644]
ESI-LOG	syslog over TLS	SP-SEC-Serv-2.3-11 - [RFC 5425] SP-SEC-Serv-2.3-25 - [RFC 9662]
ESI-DNS	DNSSEC	SP-SEC-Serv-2.3-22 - [RFC 9364]

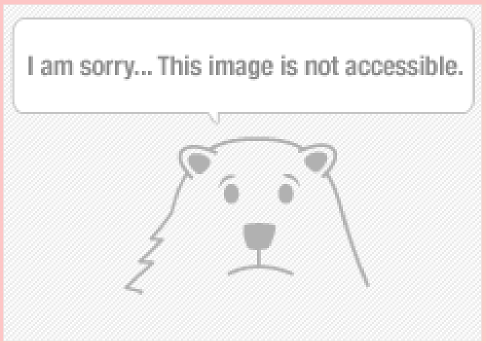
, SP-SEC-SERVServ-5-1 - The SSI-STS service is is an important Shared Cybersecurity Service, which is used to distribute common time base, which is important for all Shared Cybersecurity Services: SSIfor example for the following services described in this document:

- SCS-PKI: for certificate creation and validitationvalidation
- SSISCS-IAM: for accurate, comparable timestamps for events
- SSISCS-LOG: for accurate, comparable timestamps for log messages
- SSISCS-BKP: for accurate, comparable timestamps for backup archives

[SPPRAMSS-3828]

- SCS-UAS: for accurate, comparable timestamps for tokens

, SP-SEC-SERVServ-5.1-1 -



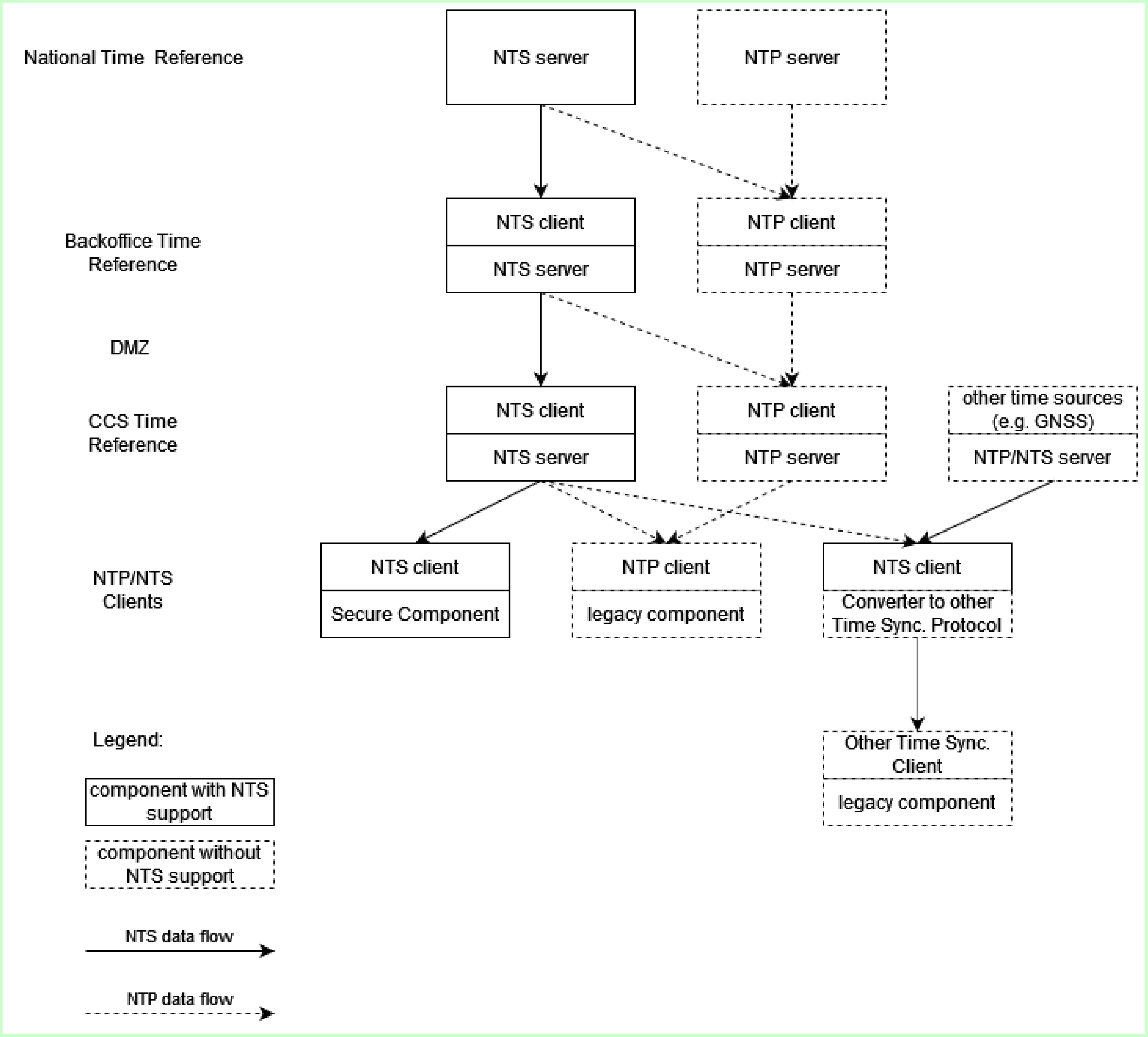


Figure 2 Exemplary hierarchy of NTS servers

[SPPRAMSS-3702]

, SP-SEC-SERVServ-5.2-1 - For resiliency, the operation of multiple time servers is recommended. [SPPRAMSS-3820]

, SP-SEC-SERVServ-5.2-2 - The SSI-STS time server shall use Network Time Security (NTS) as specified in SP-SEC-Serv-2.3-19 - [RFC 8915].

Note: This means, that at least TLS version 1.3 is used. [SPPRAMSS-9965]

, SP-SEC-SERVServ-5.2-3 - The SSI-STS time server shall use the fixed network ports defined in SP-SEC-Serv-2.3-19 - [RFC 8915].

Note: This means that NTPv4 Port Negotiation is not used. **[**SPPRAMSS-3716 **]**

, SP-SEC-SERVServ-5.2-4 - The SSI-STS time server shall use a Operator Non-Safety Communication Certificate (ONCC) as server certificate as defined in 6.2.42 - Operator Certificates. **[**SPPRAMSS-5264 **]**

, SP-SEC-SERVServ-5.2-5 - The SSI-STS time server shall only accept NTS-KE requests from authenticated clients. **[**SPPRAMSS-5266 **]**

, SP-SEC-SERVServ-5.2-6 - The SSI-STS server shall distribute Coordinated Universal Time (UTC). **[**SPPRAMSS-6724 **]**

, SP-SEC-SERVServ-5.3-1 - The SSI-STS client shall use NTS as specified in SP-SEC-Serv-2.3-19 - [RFC 8915] .

Note: This means, that at least TLS version 1.3 is used. **[**SPPRAMSS-3701 **]**

, SP-SEC-SERVServ-5.3-2 - The SSI-STS client shall send the NTS-KE requests to the configured NTS server on TCP port 4460. **[**SPPRAMSS-3717 **]**

, SP-SEC-SERVServ-5.3-3 - The SSI-STS client shall use a Operator Non-Safety Communication Certificate (ONCC) as defined in 6.2.42 - Operator Certificates for client authentication. **[**SPPRAMSS-5265 **]**

, SP-SEC-Serv-5.3-4 - During commissioning, the SSI-STS client shall use NTP as specified in SP-SEC-Serv-2.3-12 - [RFC 5905] .

Note: this removes the circular dependency when requesting the first operator certificates.

SP-SEC-SERVServ-5.4-1 - NTS is backwards compatible to NTP. That means an NTP client can synchronize with an NTS server (the NTS extension / signature appendix is ignored by NTP implementations). However, if the signatures of the time sync messages are not evaluated (in case of an NTP client), the client is vulnerable to man-in-the-middle attacks (no server authentication or message integrity protection). **[**Text, SPPRAMSS-6707 **]**

, SP-SEC-SERVServ-6-1 - 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.See also RFC 3647 and RFC 4158. **[**SPPRAMSS-3690 **]**

, SP-SEC-SERV-6-2 - Internet protocols intended to provide security for information exchange, for example TLS and OPC UA SC, use PKI certificates to authenticate communicating parties with each other as well as support encryption and integrity of the communication session. **[**SPPRAMSS-3122 **]**

, SP-SEC-SERV-6-3 - A PKI consist of several elements,

1. 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.
2. Certification Authority (CA): A trusted entity that serves authentication infrastructures as well as registering entities that need PKI. It is the organization that issues digital certificates.

3. Registration Authority (RA): Is certified by a CA and validates the identity of PKI users requesting information on a certificate.
4. Certificate Revocation List (CRL): Provides a means for checking the continued validity of certificates issued by a Certificate Authority (CA). The CRL contains the serial numbers of certificates that have been revoked before the end of their validity period, e.g. due to suspected breaches or other security concerns.

[SPPRAMSS-3124 **]**

, SP-SEC-SERV-6-4 - The following Figure depicts an example of a PKI hierarchy.

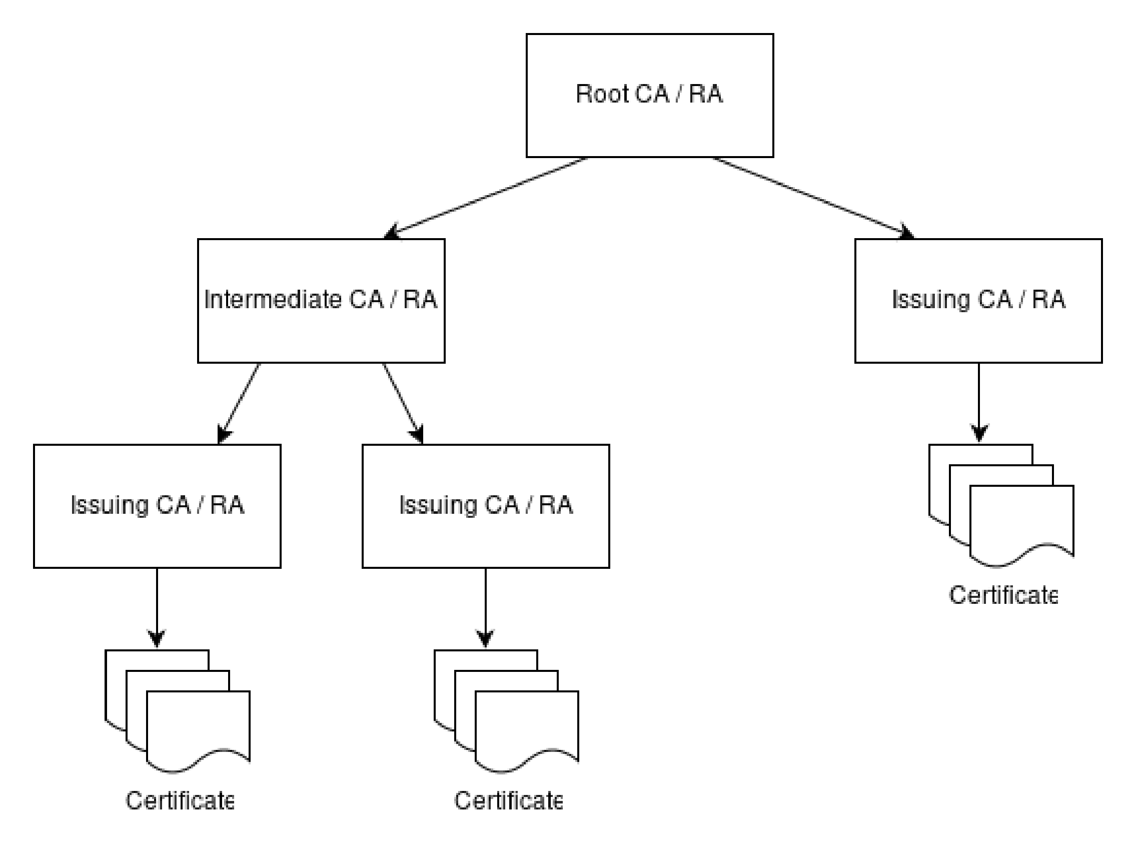


Figure 3 Example of a PKI hierarchy

[SPPRAMSS-3123 **]**

, SP-SEC-SERV-6-5 - In the Figure in SPPRAMSS-3123, CA is a Certificate Authority responsible for issuing, rekeying, and revoking digital certificates. A digital certificate contains, among others, a public key and information related to the key, its owner, its validity period, and its allowed use (for example encryption, authentication, safety-related communication, OPC UA SC communication). **[**SPPRAMSS-3125 **]**

, SP-SEC-SERV-6-6 - In the simplest scenario, certificates are issued by a Certificate Authority. More complex scenarios require the presence of a Registration Authority (RA). When a new entity wants to obtain a client certificate, it issues a request to the RA which then tries to authenticate and authorize the requester, which includes checking the device serial number. If these checks had positive outcome, the RA forwards the request to the CA, which issues the digital certificate. The RA can be a part of a CA as well as a separate entity.

[SPPRAMSS-3126 **]**

, SP-SEC-SERV-6-7 - CAs can be organized in a hierarchical tree structure with CA certificates issued by a higher-level CA. This tree structure has a single root node, called “root CA” and all clients must know and trust the root CA certificate (also called root-of-trust).

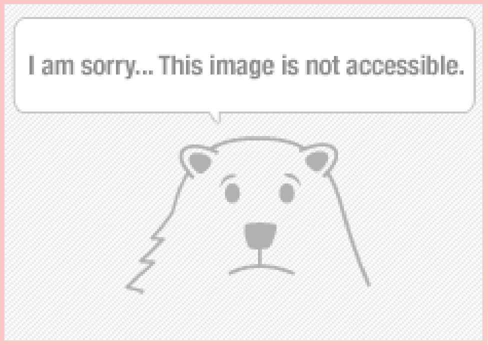
Note: A PKI client may be related to more than one root CA.

[SPPRAMSS-3392 **]**

, SP-SEC-SERV-6-8 - Digital certificates are managed using the Certificate Management Protocol (CMP) according to the Lightweight CMP Profile (LCMPP) RFC 9483 .

[SPPRAMSS-3390 **]**

, SP-SEC-SERVServ-6-92 - The following Figure shows interfaces and protocols used between the PKI and PKI users. Secure Components. The Secure Components clients establish a TLS connection using the certificates distributed by the PKI.



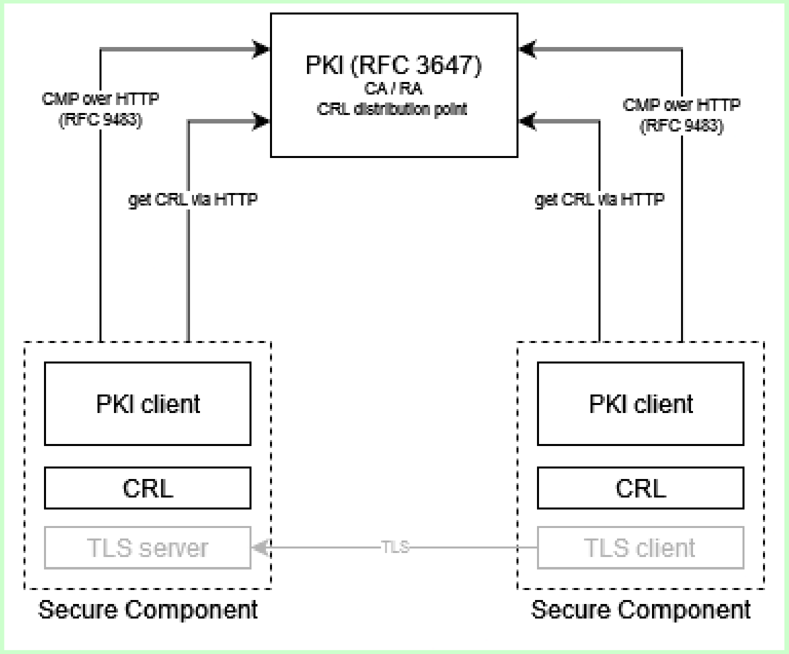


Figure 43 Interface between PKI and PKI clients

[SPPRAMSS-3393 **]**

Secure Components

, SP-SEC-SERV-6-10 - The example shown in the Figure above (SPPRAMSS-3393) shows a TLS interface using the certificates distributed by the PKI. **[**SPPRAMSS-3398 **]**

, SP-SEC-SERV-6-11 - The certificate management interface (CMP in the Figure above, SPPRAMSS-3393) between a PKI client and the PKI allows issuing and rekeying certificates of the PKI client using the CMP protocol according to the Lightweight CMP Profile (LCMPP) RFC 9483.
[SPPRAMSS-3396]

, SP-SEC-SERV-6-12 - Each certificate in a certificate chain is checked against the corresponding CRL produced by the CAs. This requires that the PKI client periodically obtains a local copy of the needed CRLs.
[SPPRAMSS-3397]

, SP-SEC-SERV-6-13 - A CRL is downloaded from the URL given by the CRL Distribution Point (CDP) extension in the respective certificate as defined in RFC 5280.

[SPPRAMSS-3394]

, SP-SEC-SERV-6-14 - In future version of this document, the ciphers for securing communication and protecting integrity will be extended to support additional cipher, e.g. for post quantum cryptography (PQC). Additional ciphers (like PQC ciphers) will be added to communication cipher requirements, the signature generation and verifying requirements and the PKI certificate profiles.
[SPPRAMSS-10107]

, SP-SEC-SERVServ-6.1.1-1 - The following Figure shows the commissioning SP-Sec-Comp-5.5.4 describes the commissioning process of new component component to an installation. The device Secure Component authenticates itself to the Registration Authority (RA) with a Manufacturer Device Certificate (MDC, see 6.2.31 - Manufacturer Certificates) to request the Operator Device Certificate (ODC, see 6.2.42 - Operator Certificates) according to RFC 9483 sections Sections 4.1.1 and 5.2.1 of SP-SEC-Serv-2.3-24 - [RFC 9483]. With the ODC, further operator certificates can be obtained according to RFC 9483 sections Sections 4.1.2 and 5.2.

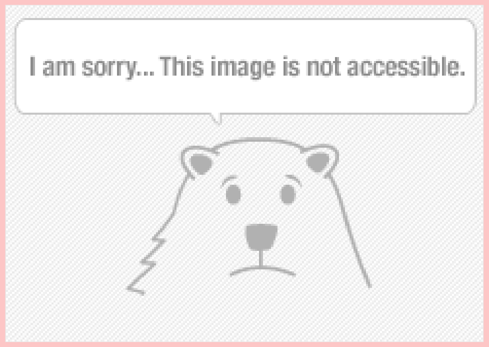
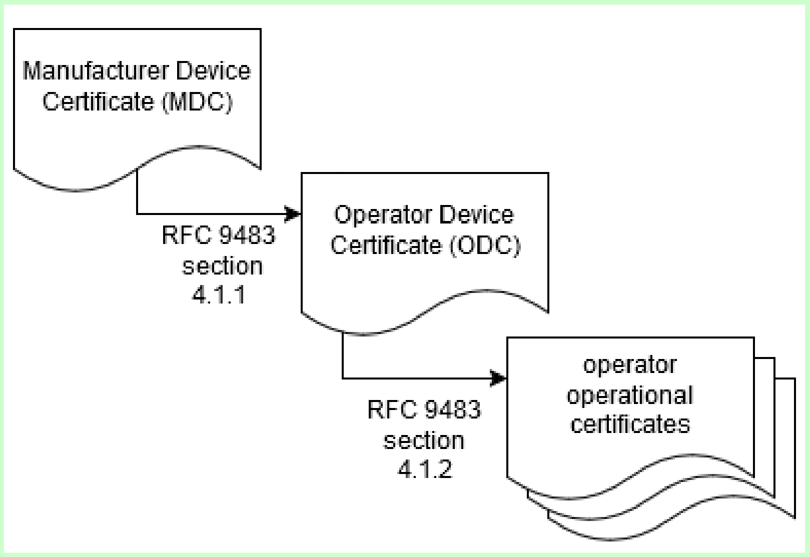


Figure 5 Overview of Certificate Commissioning
[SPPRAMSS-5086]of SP-SEC-Serv-2.3-24 - [RFC 9483].

, SP-SEC-SERV-6.1.1-2 - For a detailed description of the comissioning procedure see Chapter "PKI Commissioning Procedure" in the Secure Component Specification. [SPPRAMSS-10181]

, SP-SEC-SERVServ-6.1.2-1 - The following Figure shows the dependencies of certificates. The Certificate Management Protocol (CMP) is used to request further certificates. Thereby, the previous certificate is used to authenticate the device before requesting following certificates. Since the Manufacturer Device Certificate (MDC) is installed during manufacturing, the device always has the possibility to request the other certificates.


Manufacturer Device Certificate (MDC)
RFC 9483 section 4.1.1
Operator Device Certificate (ODC)
RFC 9483 section 4.1.2
operator operational certificates

[SPPRAMSS-5845]

, **SP-SEC-SERVServ-6.1.3-1 -** Operator Certificates can be updated before their validity ends according to SP-SEC-Serv-2.3-24 - [RFC 9483] section 4.1.3. **[**SPPRAMSS-10182 **]**

, **SP-SEC-SERVServ-6.1.4-1 -** Operator Certificates can be revoked according to SP-SEC-Serv-2.3-24 - [RFC 9483] section 5.3.2. **[**SPPRAMSS-10183 **]**

, **SP-SEC-SERVServ-6.2-1 -** The PKI CA shall issue certificates that comply to X.509 v3 as defined in SP-SEC-Serv-2.3-9 - [RFC 5280. **[**SPPRAMSS-9990 **]**] .

, **SP-SEC-SERVServ-6.2-2 -** All certificates in the PKI hierarchy shall be based on Elliptic Curve Cryptography (ECC). **[**SPPRAMSS-10177 **]**

Note: In future version of this document, the cryptographic primitives for the PKI will be extended to support additional primitives, e.g. for post quantum cryptography (PQC).

, **SP-SEC-SERV-6.2-3 -** If support for RSA is required for backwards compatibility to OPC Profile Group UACore 1.04, additional certificates can also be based on RSA.

Note: This requirement will be removed in a future version of this specification. **[**SPPRAMSS-10178 **]**

, **SP-SEC-SERVServ-6.2.1-13 -** The PKI certificate profiles (see 14.1 - Certificate Profiles) use the following rail-specific Object Identifiers (OIDs) defined in SP-SEC-Serv-2.3-26 - [RFC automation-keyusages] in the Extended Key Usage (EKU) field.

OID	Name	Description
`1.3.6.1.4.1.4329.44.1.1`	`configSigning`	Used in critical Extended Key Usage field of Manufacturer Configuration Signer Certificate (MCSC) and Operator Configuration Signer Certificate (OCSC) to denote the use of the certificate for signing configuration files.

OID	Name	Description
`1.3.6.1.4.1.4329.44.1.2`	`trustanchorSigning`	Used in critical Extended Key Usage field of Manufacturer Trust Anchor Signer Certificate (MTASC) and Operator Trust Anchor Signer Certificate (OTASC) to denote the use of the certificate for signing trust anchor configuration files.
`1.3.6.1.4.1.4329.44.1.3`	`updateSigning`	Used in critical Extended Key Usage field of Manufacturer Update Signer Certificate (MUSC) to denote the use of the certificate for signing software or firmware update packages.
`1.3.6.1.4.1.4329.44.1.100`	`safetyCommunication`	Used in critical Extended Key Usage field of Operator Safety Communication Certificate (OSCC) to denote the use of the certificate for safety-critical communication.

Object Identifier (OID) Name and Value	Description

`id-kp-configSigning`
`1.3.6.1.5.5.7.3.41`
	Used in critical Extended Key Usage field of Manufacturer Configuration Signer Certificate (MCSC) and Operator Configuration Signer Certificate (OCSC) to denote the use of the certificate for verifying signatures of general-purpose configuration files.

`id-kp-trustAnchorConfigSigning`
`1.3.6.1.5.5.7.3.42`
	Used in critical Extended Key Usage field of Manufacturer Trust Anchor Signer Certificate (MTASC) and Operator Trust Anchor Signer Certificate (OTASC) to denote the use of the certificate for verifying signatures of trust anchor configuration files. Trust anchor configuration files are used to add or remove trust anchors to the trust store of a Secure Device.

`id-kp-updatePackageSigning`
`1.3.6.1.5.5.7.3.43`
	Used in critical Extended Key Usage field of Manufacturer Update Signer Certificate (MUSC) to denote the use of the certificate for verifying signatures of secure software or firmware update packages.

`id-kp-safetyCommunication`
`1.3.6.1.5.5.7.3.44`
	Used in critical Extended Key Usage field of Operator Safety Communication Certificate (OSCC) to denote the use for authenticating a communication peer for safety-critical communication

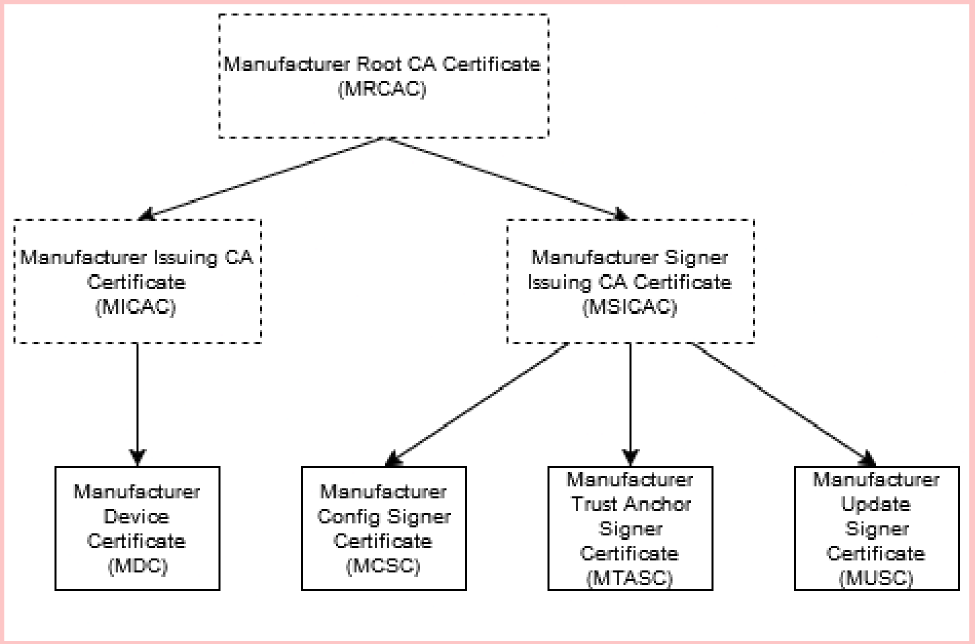
[SPPRAMSS-7128]Note: The EKU OIDs are registered in SP-SEC-Serv-2.3-3 - [IANA SMI PKIX EKU]

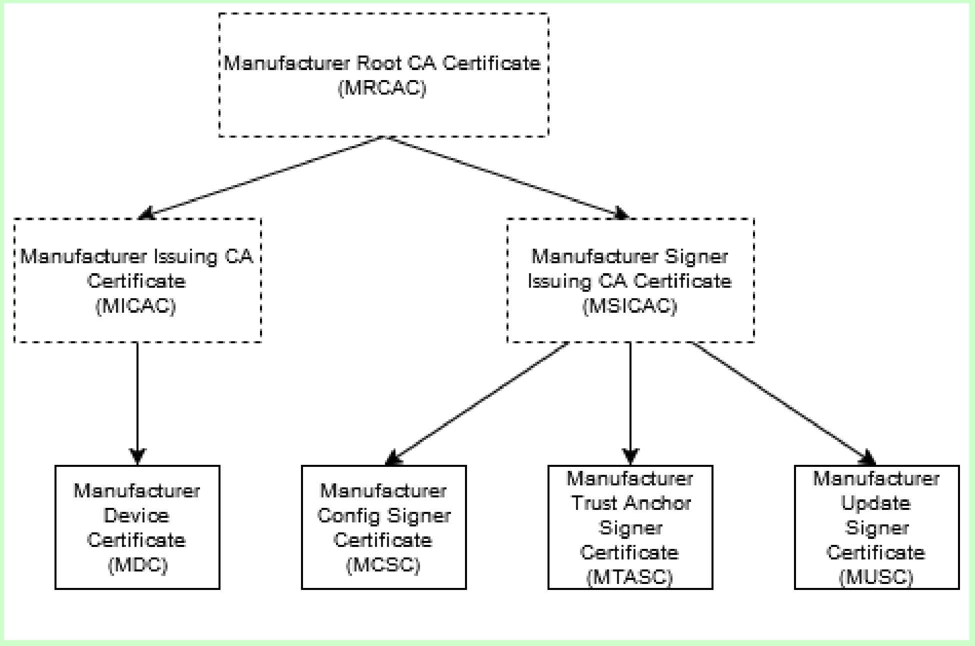
, SP-SEC-SERV-6.2.2-1 - A CRL shall contain the nextUpdate field.

Note: recommended update period is 24h. [SPPRAMSS-7629]

, SP-SEC-SERVServ-6.2.31-1 - The following Figure shows an example of a PKI hierarchy for railway manufacturers. All certificates are based on Elliptic Curve Cryptography (ECC). While this section includes requirements for the leaf certificates (MDC, MCSC, MTASC, MUSC), the exact numbers and characteristics of root and issuing CAs can be defined by the manufacturer. [SPPRAMSS-5650]

Note: trust anchors are usually associated with a root CA, but this is not a requirement


Manufacturer Root CA Certificate (MRCAC)
Manufacturer Issuing CA Certificate (MICAC)
Manufacturer Signer Issuing CA Certificate (MSICAC)
Manufacturer Device Certificate (MDC)
Manufacturer Config Signer Certificate (MCSC)
Manufacturer Trust Anchor Signer Certificate (MTASC)
Manufacturer Update Signer Certificate (MUSC)



Manufacturer Root CA Certificate (MRCAC)
Manufacturer Issuing CA Certificate (MICAC)
Manufacturer Signer Issuing CA Certificate (MSICAC)
Manufacturer Device Certificate (MDC)
Manufacturer Config Signer Certificate (MCSC)
Manufacturer Trust Anchor Signer Certificate (MTASC)
Manufacturer Update Signer Certificate (MUSC)

Figure 64 Manufacturer PKI Hierarchy. Certificates with solid lines have are defined by certificate profiles.

, SP-SEC-SERVServ-6.2.31-2 - The following table lists the leaf certificates issued by the manufacturer and their use case.

Table 2 Overview of manufacturer leaf certificates and their usage.

Certificate Name	Certificate Tag	Use Case	Usual OccurenceOccurrence
Manufacturer Device Certificate	MDC	The MDC uniquely identify every device in the scope of the manufacturer.	one MDC per device
Manufacturer Config Signer Certificate	MCSC	The MCSC is used by the manufacturer to sign configuration files.	one MCSC per manufacturer

Certificate Name	Certificate Tag	Use Case	Usual OccurenceOccurrence
Manufacturer Trust Anchor Signer Certificate	MTASC	The MTASC is used by the manufacturer to add trusted operator root CA certificates 💬 to a device.	one MTASC per manufacturer
Manufacturer Update Signer Certificate	MUSC	The MUSC is used by the manufacturer to sign SW/FW update files.	one MUSC per manufacturer

[SPPRAMSS-7675]

, SP-SEC-SERV-6.2.3-3 - Any complete certificate chain of the manufacturer shall contain at least three certificates: root CA certificate, issuing CA certificate, and leaf certificate. **[SPPRAMSS-5652]**

, SP-SEC-SERVServ-6.2.1-3 -4 - The Manufacturer Device Certificate (MDC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.1-1. **[SPPRAMSS-7645]**

, SP-SEC-SERVServ-6.2.31-54 - The Manufacturer Config Signer Certificate (MCSC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.1-2. **[SPPRAMSS-7356]**

, SP-SEC-SERVServ-6.2.31-65 - The Manufacturer Trust Anchor Signer Certificate (MTASC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.1-3. **[SPPRAMSS-7404]**

, SP-SEC-SERVServ-6.2.31-76 - The Manufacturer Update Signer Certificate (MUSC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.1-4. **[SPPRAMSS-7405]**

, SP-SEC-SERVServ-6.2.42-1 - The following Figure shows an example of a PKI hierarchy for railway operators. All certificates are based on Elliptic Curve Cryptography (ECC). While this section includes requirements for the leaf certificates (ODC, ONCC, OSCC, OHUC, OTUC, OCSC, OTASC), the exact numbers and characteristics of root and issuing CAs can be defined by the operator.

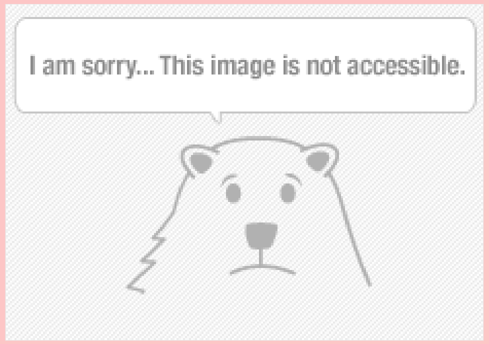


Figure 7Note: trust anchors are usually associated with a root CA, but this is not a requirement

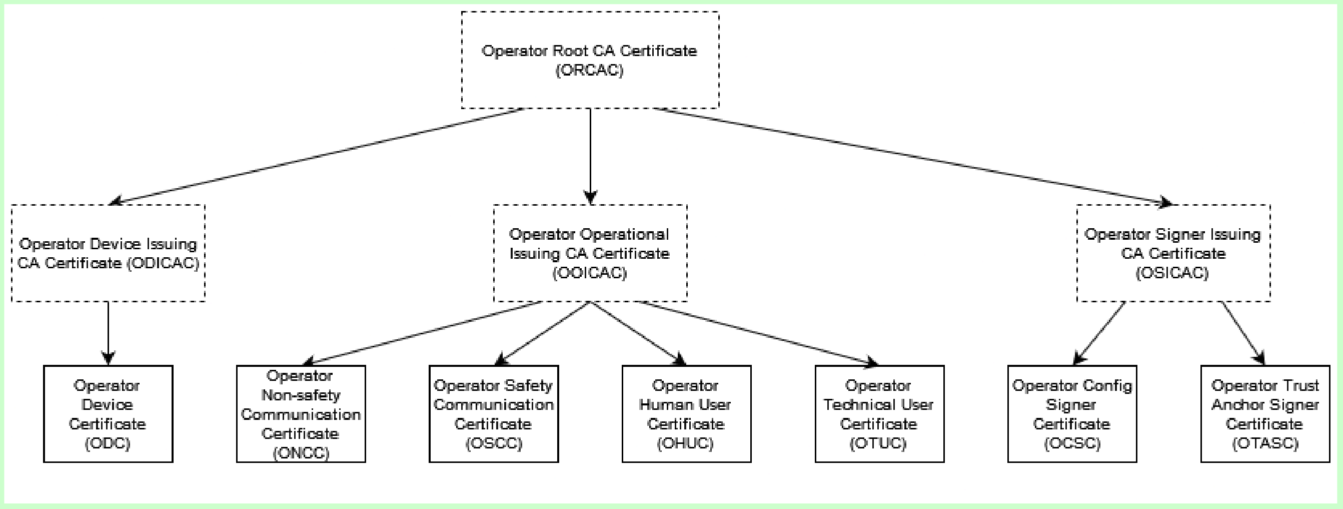

Operator Root CA Certificate (ORCAC)
Operator Device Issuing CA Certificate (ODICAC)
Operator Operational Issuing CA Certificate (OOICAC)
Operator Signer Issuing CA Certificate (OSICAC)
Operator Device Certificate (ODC)
Operator Non-safety Communication Certificate (ONCC)
Operator Safety Communication Certificate (OSCC)
Operator Human User Certificate (OHUC)
Operator Technical User Certificate (OTUC)
Operator Config Signer Certificate (OCSC)
Operator Trust Anchor Signer Certificate (OTASC)

Figure 5 Operator PKI Hierarchy (ECC). Certificates with solid lines are defined by certificate profiles.

[SPPRAMSS-5126]

, SP-SEC-SERVServ-6.2.42-2 - The following table lists the leaf certificates issued by the operator and their use case.

Table 3 Overview of operator leaf certificates and their usage.

Certificate Name	Certificate Tag	Use Case	Usual OccurenceOccurrence
Operator Device Certificate	ODC	The ODC uniquely identify every device within the scope of the operator.	one ODC per device
Operator Non-safety Communication Certificate	ONCC	ONCCs are used to protect non-safety communication.	zero to multiple ONCCs per device
Operator Safety Communication Certificate	OSCC	OSCCs are used to protect safety communication.	zero to multiple OSCCs per device
Operator Human User Certificate	OHUC	OHUCs are used by human users, e.g. for authentication and authorisation.	zero to multiple OHUCs per human user
Operator Technical User Certificate	OTUC	OTUCs are used by software processes, e.g. for authentication and authorisation.	zero to multiple OTUCs per human userper software process
Operator Config Signer Certificate	OCSC	The OCSC is used by the operator to sign configuration files.	one OCSC per operator
Operator Trust Anchor Signer Certificate	OTASC	The OTASC is used by the operator to add trusted operator root CA certificates to a device. These certificates can be owned by the same operator or a different one.	one OTASC per operator

[SPPRAMSS-7676]

, **SP-SEC-SERV-6.2.4-3 -** Any full certificate chain in the PKI hierarchy of the operator shall contain at least three certificates: root CA certificate, issuing CA certificate, and leaf certificate. **[**SPPRAMSS-7646 **]**

, **SP-SEC-SERVServ-6.2.42-43 -** The Operator Device Certificate (ODC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-1. **[**SPPRAMSS-8001 **]**

, **SP-SEC-SERVServ-6.2.2-4 -5 -** The Operator Non-Safety Communication Certificate (ONCC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-2. **[**SPPRAMSS-5129 **]**

, **SP-SEC-SERVServ-6.2.42-65 -** The Operator Safety Communication Certificate (OSCC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-3. **[**SPPRAMSS-5131 **]**

, **SP-SEC-SERVServ-6.2.42-76 -** If more than one connection network interface is used for one safety communication, dedicated OSCCs shall be used for each connectionnetwork interface.

NOTENote : this ensures that if one the communication certificate of one network interface is renewed, the connection over the other connection network interface maintains its independency.

[SPPRAMSS-6681]

, **SP-SEC-SERVServ-6.2.42-87 -** The Operator Human User Certificate (OHUC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-4. **[**SPPRAMSS-5123 **]**

, **SP-SEC-SERVServ-6.2.42-98 -** The OHUC shall be delivered with initial protection (e.g. passphrase or PIN) which can be changed by the user.

[SPPRAMSS-6589]

, **SP-SEC-SERVServ-6.2.42-109 -** The Operator Technical User Certificate (OTUC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-5. **[**SPPRAMSS-5137 **]**

, **SP-SEC-SERVServ-6.2.42-1110 -** The Operator Configuration Signer Certificate (OCSC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-6. **[**SPPRAMSS-5270 **]**

, **SP-SEC-SERVServ-6.2.42-1211 -** The Operator Trust Anchor Signer Certificate (OTASC) shall fulfill the certificate profile defined in SP-SEC-SERVServ-1314.1.2-7 **[**SPPRAMSS-9943 **]**

, **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-SERVServ-6.3-12 -** The SSI-PKI shall issue X.509 v3 certificates according to SPPRAMSS-2031 - as defined in SP-SEC-Serv-2.3-9 - [RFC 5280]. **[**SPPRAMSS-6744 **]**

, **SP-SEC-SERVServ-6.3-23 -** The SSI-PKI shall issue certificates according to the certificate profiles defined in SPPRAMSS-5087 - Use Case: Updating Operator Certificates. **[**SPPRAMSS-6745 **]**14.1 - Certificate Profiles.

, **SP-SEC-SERVServ-6.3-34 -** 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) [RFC9483as defined in SP-SEC-Serv-2.3-24 - [RFC 9483].

[SPPRAMSS-4062]

, **SP-SEC-SERVServ-6.3-45 -** 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). [SPPRAMSS-4064]

, **SP-SEC-SERVServ-6.3-56 -** The PKI RA/CA shall validate the content and signature-based message protection of every received CMP request according to LCMPP Section 3.5 in SP-SEC-Serv-2.3-24 - [RFC 9483] before accepting it. Any error condition shall be handled according to LCMPP Section 3.6.2. [SPPRAMSS-6604]

, **SP-SEC-SERVServ-6.3-67 -** The PKI RA/CA shall issue and rekey certificates compliant to the certificate profiles defined in 13.1 - Certificate Profiles.

[SPPRAMSS-4065]

handle errors according to Section 3.6.2 of SP-SEC-Serv-2.3-24 - [RFC 9483].

, **SP-SEC-SERVServ-6.3-78 -** The PKI RA/CA shall provide CRLs compliant to RFC 6818 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. [SPPRAMSS-4063]

, **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-SERVServ-6.3-810 -** The PKI RA/CA shall not grant any request for implicit confirmation and shall send a pkiConf message at the reception of the certConf message.

[SPPRAMSS-4142]Note: this means that ImplicitConfirm is not used.

, **SP-SEC-SERV-6.3-9 -** If the PKI RA does not receive a certConf message from a PKI client after sending a Initialization Response (ip), Certification Response (cp), or Key Update Response (kup) message or if the received certConf message contains the status “rejection”, the PKI RA shall revoke the certificate corresponding to the original request by sending a Revocation Request (rr) according to LCMPP Section 5.3.2 to the PKI CA. [SPPRAMSS-6573]

, **SP-SEC-SERVServ-6.3-1011 -** The PKI RA/CA shall provide the following CMP endpoints according to Section 6.1 of LCMPP 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
`/.well-known/cmp/p/ODC/initialization`	ODC	CMP requests: message protection with MDC CMP responses: message protection with issuing CA key
`/.well-known/cmp/p/ONCC/certification`	ONCC	CMP message protection with ODC CMP responses: message protection with issuing CA key

CMP Endpoint URL	Issued Certificate Types	Endpoint Protection
`/.well-known/cmp/p/OSCC/certification`	OSCC	CMP message protection with ODC CMP responses: message protection with issuing CA key

[SPPRAMSS-5167]

, **SP-SEC-SERVServ-6.3-1112 -** The PKI RA/CA shall provide the following CMP endpoints according to Section 6.1 of LCMPP for 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
`/.well-known/cmp/p/ODC/keyupdate`	ODC	CMP requests: message protection with ODC CMP responses: message protection with issuing CA key
`/.well-known/cmp/p/ONCC/keyupdate`	ONCC	CMP message protection with ONCC CMP responses: message protection with issuing CA key
`/.well-known/cmp/p/OSCC/keyupdate`	OSCC	CMP message protection with OSCC CMP responses: message protection with issuing CA key

[SPPRAMSS-5168]

, **SP-SEC-SERVServ-6.3-1213 -** 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 LCMPP.

[SPPRAMSS-5186]

SP-SEC-Serv-2.3-24 - [RFC 9483]: Initialization Request (ir), Certification Request (cr), and Revocation Request (rr).

, **SP-SEC-SERVServ-6.3-1314 -** The PKI RA shall only forward correctly authenticated and authorized CMP requests (see LCMPP 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-SERVServ-6.3-1011 and SP-SEC-SERVServ-6.3-1112).

[SPPRAMSS-5223]

, **SP-SEC-SERVServ-6.3-1415 -** The PKI CA shall only accept CMP requests if they are correctly signed by the RA's ONCC see LCMPP Sections 3SP-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 pre-configured preconfigured value.

[SPPRAMSS-5188]

, **SP-SEC-SERVServ-6.3-1516 -** 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 [RFC9481SP-SEC-Serv-2.3-23 - [RFC 9481].

Note: SP-SEC-SERVServ-6.3-1011 and SP-SEC-SERVServ-6.3-1112 define which key to use for every CMP endpoint.

[SPPRAMSS-7494]

, SP-SEC-SERVServ-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 (LCMPP) [RFC9483].

[SPPRAMSS-4070]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-SERVServ-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] Section 4.1.1) and the CMP Certification Request message (cr) and certConf with ODC (SP-SEC-Serv-2.3-24 - [RFC 9483 section] Section 4.1.2) according to SP-SEC-SERVServ-6.3-1011.

[SPPRAMSS-6602]

, SP-SEC-SERVServ-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 sction] Section 4.1.3). [SPPRAMSS-7177]

, 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-SERVServ-6.4-45 - The SSI-PKI client shall sign CMP requests by using ecdsa-with-sha256 as protectionAlg as defined in section Section 3.2 of SP-SEC-Serv-2.3-23 - [RFC 9481] .

[SPPRAMSS-7496]

, SP-SEC-SERVServ-6.4-56 - 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 inf in SP-SEC-Serv-2.3-24 - [RFC 9483] .

[SPPRAMSS-4068]

, SP-SEC-SERVServ-6.4-67 - 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] section 3.5 before accepting it.

Note: Any error condition should be handled according to SP-SEC-Serv-2.3-24 - [RFC 9483 section] Section 3.6.1. [SPPRAMSS-9670]

, SP-SEC-SERVServ-6.4-78 - The SSI-PKI client shall request and rekey certificates compliant to the certificate profiles defined in [SPPRAMSS-4069]needed for operation.

, SP-SEC-SERVServ-6.4-89 - The SSI-PKI client shall download CRLs via HTTP and process CRLs via HTTP as defined in SP-SEC-Serv-2.3-9 - [RFC 5280 using the] using a URL defined in the CRL Distribution Point (CDP) extension. [SPPRAMSS-4067], which can be overwritten by a URL defined in the client's configuration.

, SP-SEC-SERVServ-6.4-910 - The PKI client shall send a certConf message at the reception of the ip, cp, or kup message according to LCMPP Section SP-SEC-Serv-2.3-24 - [RFC 9483] Section 4.1.1.

[SPPRAMSS-4141]

, SP-SEC-SERVServ-6.4-1011 - 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 [RFC9481SP-SEC-Serv-2.3-23 - [RFC 9481].
Note: SP-SEC-SERVServ-6.3-1011 and SP-SEC-SERVServ-6.3-1112 define which key to use for every CMP endpoint.
[SPPRAMSS-7495 **]**

SP-SEC-SERVServ-7-1 - The SSI-IAM is a service an interface for managing digital identities (humans or machines) centrallyhuman users, software processes or devices). This eleminates eliminates the need for credential stores on individual components. The IAM acts as as a single source of truth for identification and authorisation. **[**Text, SPPRAMSS-4974 **]**authorisation. Beyond usage of SSI-IAM by other Shared Cybersecurity Services as defined in this specification, the SCS-IAM is only used by SDI/SMI.

, SP-SEC-SERVServ-7-2 - The SSI-IAM server shall have the possibility to retrieve identities from an identity store (e.g. an HR system for humans or an asset management system for machines). **[**SPPRAMSS-4975 **]**

, SP-SEC-SERVServ-7-3 - The SSI-IAM server shall have the capability to retrieve authorisation information from an authorisation store (e.g. a training database for maintainers). **[**SPPRAMSS-4976 **]**

, SP-SEC-SERVServ-7-4 - The OPCC UA permissions for OPC UA SSI are defined in the Secure Communication Specification, Chapter 5 . **[**SPPRAMSS-9806 **]**of the SP-SEC-Serv-2.3-28 - [SP-SEC-CommSpec].

, SP-SEC-SERVServ-7-5 - The SSI-IAM interface is used to query and manage assets and human users. The interface is involved in multiple use cases such as the verification of initial certificate requests, certificate storage, and network authentication.
[SPPRAMSS-7970 **]**

, SP-SEC-SERVServ-7-6 - The SSI-IAM server shall accept SCIM 2.0 requests over REST over HTTPS according to RFC 7644, RFC 7230 and RFC 7231. **[**SPPRAMSS-5803 **]**
SP-SEC-Serv-2.3-15 - [RFC 7644].

, SP-SEC-SERVServ-7-7 - For the HTTPS session, the SSI-IAM acting as a server shall use an Operator Non-safety Communication Certificate (ONCC) or Manufacturer Device Certificate (MDC), if no ONCC is available. **[**SPPRAMSS-5811 **]**

, SP-SEC-SERVServ-7-8 - The SSI-IAM server shall send SCIM 2.0 JSON-formatted responses as defined in SP-SEC-Serv-2.3-15 - [RFC 7644]. **[**SPPRAMSS-5802 **]**

, SP-SEC-SERVServ-7-9 - The SSI-IAM server shall send SCIM 2.0 responses following the Core Schema defined in SP-SEC-Serv-2.3-14 - [RFC 7643. **[**SPPRAMSS-10351 **]**] .

, SP-SEC-Serv-7-10 - The SCS-IAM server shall be able to synchronise its asset database via ESI-IAM with an asset management system.

, SP-SEC-Serv-7-11 - The SCS-IAM server shall be able to synchronise its user database via ESI-IAM with a corporate directory.

, **SP-SEC-SERVServ-7.1-1 -** The SSI-IAM server shall provide access to its asset inventory via SCIM 2.0 under the endpoint `/v2/Assets`. [SPPRAMSS-9814]

, **SP-SEC-Serv-7.1-2 -** The SSI-IAM server shall enforce the following permissions for its asset inventory:

Permission Name	Description
`eu.rail.security.iam.asset-info`	This permission allows to check if a given asset (defined by serial number and manufacturerDN) exists in the asset database (see SP-SEC-Serv-7.1-4)
`eu.rail.security.iam.update-assets-certificates`	This permission allows to modify the certificates (add, delete, update operations) of a given asset (see SP-SEC-Serv-7.1-9)

, **SP-SEC-SERVServ-7.1-23 -** The SSI-IAM server shall distinguish the following Secure Components Component types by matching the serial number from their MDC or the CN from their ODC to the IAM's asset database : PKI RA, NAC, Update Server. [SPPRAMSS-9807]and assign the following permissions:

Secure Component Type	Permissions
PKI RA	`eu.rail.security.iam.asset-info` `eu.rail.security.iam.update-assets-certificates`
NAC	`eu.rail.security.iam.asset-info`
Update Server (as defined by SMI)	`eu.rail.security.iam.asset-info`

Note: mapping these permissions to roles, which match to component types is allowed

, **SP-SEC-SERV-7.1-3 -** If the SSI-IAM server recieves a SCIM request from a Secure Component for `/v2/Assets`, the SSI IAM shall allow the actions defined in the following table based on the type of the Secure Component that send the request:

Secure Component Type	Action: read assets (HTTP GET)	Action: update assets certificates
PKI RA	allowed	allowed
SSI-NAC	allowed	disallowed
Update Server (SMI)	allowed	disallowed
all other types	disallowed	disallowed

[SPPRAMSS-9808]

, **SP-SEC-SERVServ-7.1-4 -** The servers implementing SSI-PKI RA, SSI-NAC or Update Server (according to SMI) shall support the ability to check if an asset is known to the SSI-IAM and active by sending the following an HTTP GET request to the SSI-IAM interface with a filter that includes the either serial number from the MDC (as `cn` `serialNumber`attribute) of this asset and the DN of the manufacturer root CA certificate (as `manufacturerDN` attribute) or the CN from the ODC (as `CN`attribute) of this asset.

Note1: a MDC-based request has the following form:

```
GET /v2/Assets?filter=(cn serialNumber eq "[serial number]") and (manufacturerDN eq "[manufacturer-specific
DN]")&attributes=cn serialNumber HTTP/1.1

Host: [SSI-IAM instance address]

User-Agent: [SSI-IAM REST Client identifier]

Accept: application/scim+json [SPPRAMSS-5805 ]
```

Note2: an ODC-based request has the following form:

```
GET /v2/Assets?filter=(CN eq "[CN]")&attributes=CN HTTP/1.1

Host: [SSI-IAM instance address]

User-Agent: [SSI-IAM REST Client identifier]

Accept: application/scim+json
```

, SP-SEC-SERVServ-7.1-5 - If the SSI-IAM server receives a request for a known asset by serial number, the SSI-AM IAM server shall check if an asset with the requested serial number exists in the IAM's database and , the DN in the manufacturer certificate matches the root stored in the IAM . **[**SPPRAMSS-6708 **]**and the assets state is active.

, SP-SEC-Serv-7.1-6 - If the SSI-IAM server receives a request for a known asset by CN, the SSI-IAM server shall check if an asset with the requested CN exists in the IAM's database and the assets state is active.

, SP-SEC-SERVServ-7.1-67 - If the SSI-IAM server has a record of the requested asset, the SSI-IAM server shall return an HTTP 200 response of the a SCIM response with the schema `urn:ietf:params:scim:api:messages:2.0:ListResponse`, containing `Resources` of the schema `urn:ietf:params:scim:core:2.0:Asset`, which includes the `serialNumber` or `CN` attribute as asset identifier.

Note1: such a response has the following form:

```
HTTP/1.1 200 OK

Content-Type: application/scim+json

{

        "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],

        "totalResults":1,

        "Resources": [

        {

                "id":"2819c223-7f76-453a-919d-413861904646",
                "schemas":["urn:ietf:params:scim:core:2.0:Asset"],

                "externalId":"device12",

                "meta":{

                      "resourceType":"Asset",

                      "created":"2011-08-01T18:29:49.793Z",

                      "lastModified":"2011-08-01T18:29:49.793Z",

                      "location":
                      "https://example.com/v2/Assets/2819c223-7f76-453a-919d-13861904646",

                      "version":"W\/\"f250dd84f0671c3\""

                },

                "
cn
                serialNumber":"<asset identifier>",

                "CN":"<asset identifier>"

              ],

        }

        ]

}
```

NoteNote2: additional attributes are allowed **[**SPPRAMSS-9842 **]**

, SP-SEC-SERVServ-7.1-78 - If the SSI-IAM has no record of the requested asset, the SSI-IAM server shall return an HTTP response with the an HTTP 404 (Not Found) error code. **[**SPPRAMSS-6709 **]**

Note: such a response has the following form:

```
HTTP/1.1 404 Not Found

Content-Type: application/scim+json

{

     "schemas": ["urn:ietf:params:scim:api:messages:2.0:Error"],

     "detail":"Resource 2819c223-7f76-453a-919d-413861904646 not found",

     "status": "404"

}
```

, SP-SEC-SERVServ-7.1-89 - The PKI Registration Authority (PKI RA) server implementing SSI-PKI shall support the ability to add issued certificates to an existing asset resource in the SSI-IAM service by sending an HTTP PATCH

SCIM request of the form shown in SPPRAMSS-6711 - HTTP Patch request for storing certificates. **[**SPPRAMSS-6710 **]**

with the schema `urn:ietf:params:scim:api:messages:2.0:PatchOp` and add the following values to the request:

- certificate type (according to 6.3 - PKI CA/RA requirements) as "type"
- certificate status "issued" or "revoked" as "status"
- certificate's Common Name as "cn"

- certificate content as base64-encoded in DER format as "value"

Note1: such a request has the following form:

```
PATCH /v2/Assets/<asset identifier> HTTP/1.1

Host: <SSI-IAM instance address>

User-Agent: <IAM REST Client identifier>

Accept: application/scim+json

Content-Type: application/scim+json

{

      "schemas":["urn:ietf:params:scim:api:messages:2.0:PatchOp"],

      "operations":[{

            "op":"add",

            "value":{

                  "certificates":[

                  {
                        "type":"<certificate type>",

                        "status":"<certificate status>",

                        "cn": "<CN of certificate>",

                        "value":"<certificate>"

                  }]

            }

      }]


}
```

Note2: additional attributes are allowed

, SP-SEC-SERV-7.1-9 - When storing a certificate in an asset resource in the SSI-IAM service, the PKI RA shall specify the certificate type according to chapter 6.3.2.3 as shown in SPPRAMSS-6711 - HTTP Patch request for storing certificates. **[**SPPRAMSS-6714 **]**

, SP-SEC-SERV-7.1-10 - When storing a certificate in an asset resource in the SSI-IAM service, the PKI RA shall specify the certificate status to "issued" or "revoked" as shown in SPPRAMSS-6711 - HTTP Patch request for storing certificates. **[**SPPRAMSS-6712 **]**

, SP-SEC-SERV-7.1-11 - When storing a certificate in an asset resource in the SSI-IAM service, the PKI RA shall add the certificate content as base64-encoded in DER format as "value" as shown in SPPRAMSS-6711 - HTTP Patch request for storing certificates. **[**SPPRAMSS-6713 **]**

, SP-SEC-SERV-7.1-12 - HTTP Patch request for storing certificates.

```
PATCH /v2/Assets/<asset identifier> HTTP/1.1
Host: <SSI-IAM instance address>
User-Agent: <IAM REST Client identifier>
Accept: application/scim+json
Content-Type: application/scim+json
{
     "schemas":["urn:ietf:params:scim:api:messages:2.0:PatchOp"],
     "operations":[{
          "op":"add",
          "value":{
               "certificates":[
               {
                    "type":"<certificate type>",
                    "status":"<certificate status>",
                    "cn": "<CN of certificate>",
                    "value":"<certificate>"
               }]
          }
     }]

}
```

Note: additional attributes are allowed **[**SPPRAMSS-6711 **]**

, SP-SEC-SERVServ-7.1-1310 - "schemas":["If the SSI-IAM successfully added the supplied certificate to the assets resource, the SSI-IAM shall return an HTTP 200 response of the following form:

HTTP/1.1 200 OK

Content-Type: application/scim+json

{

a SCIM response with the schema `urn:ietf:params:scim:api:messages:2.0:ListResponse`"],

"totalResults":1,

"Resources": [

{

"id":"2819c223-7f76-453a-919d-413861904646",

"schemas":["urn:ietf:params:scim:core:2.0:Asset"],

"externalId":"device12",

"meta":{

"resourceType":"Asset",

"created":"2011-08-01T18:29:49.793Z",

"lastModified":"2011-08-01T18:29:49.793Z",

"location":
"https://example.com/v2/Assets/2819c223-7f76-453a-919d-13861904646",

"version":"W\/\"f250dd84f0671c3\""

},

"cn":"<asset identifier>"

],

}

]

}

Note: additional attributes are allowed **[**SPPRAMSS-6715 **]**
as defined in SP-SEC-Serv-7.1-7

, **SP-SEC-SERV-7.1-14 -** If the SSI-IAM service could not add the supplied certificate to the assets resource, the SSI-IAM shall return an appropriate HTTP error according to the exact error reason. **[**SPPRAMSS-6716 **]**

, **SP-SEC-SERV-7.1-15 -** The SCS-IAM shall synchronise its user database via ESI-IAM with a Corporate Directory using SCIM 2.0. **[**SPPRAMSS-7974 **]**

, **SP-SEC-SERVServ-7.2-1 -** The SSI-IAM shall provide access to its user inventory via SCIM under the endpoint `/v2/Users`. **[**SPPRAMSS-9815 **]**

, **SP-SEC-SERVServ-7.2-2 -** If the The SSI-IAM recieves a SCIM request from a Secure Component for `/v2/Users`, the SSI IAM shall allow all Secure Components reading the user inventory. **[**SPPRAMSS-9816 **]**shall enforce the following permissions for its user inventory:

Permission Name	Description
`eu.rail.security.iam.read-permissions`	This permission allows to retrieve all permissions for a single user specified by their email address (see SP-SEC-Serv-7.2-4)

, **SP-SEC-Serv-7.2-3 -** The SSI-IAM shall assign the following permissions:

Secure Component Type	Permissions
all component types	`eu.rail.security.iam.read-permissions`

Note: mapping these permissions to roles, which match to component types is allowed

, **SP-SEC-SERVServ-7.2-34 -** The SSI-IAM client shall support the ability to retrieve user permissions from the SSI-IAM by sending the following an HTTP GET request to the SSI-IAM interface with a filter that includes the email adress address of the user as identifier.

Note: such a request has the following form:

```
GET /v2/Users?filter=emails.value eq "[user email]"&attributes=emails.value,permissions cn HTTP/1.1

Host: [SSI-IAM instance address]

User-Agent: [SSI-IAM REST Client identifier]

Accept: application/scim+json
```

[SPPRAMSS-9817 **]**

, **SP-SEC-SERVServ-7.2-45 -** If the SSI-IAM can provide the requests requested user permission, it shall return an HTTP 200 response of the permissions, the SSI-IAM server shall return a SCIM response with the schema `urn:ietf:params:scim:api:messages:2.0:ListResponse`, containing `Resources` of the schema `urn:ietf:params:scim:core:2.0:User`, which includes the users email addresses as values in the "emails" resource and the users permissions as values in the "entitlements" resource.

Note1: such a response has the following form:

```
HTTP/1.1 200 OK

Content-Type: application/scim+json

{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":1,
    "Resources": [
    {
        "id":"2819c223-7f76-453a-919d-413861904646",
        "schemas":["urn:ietf:params:scim:core:2.0:User"],
        "externalId":"jbloggs",
        "meta":{
            "resourceType":"User",
            "created":"2011-08-01T18:29:49.793Z",
            "lastModified":"2011-08-01T18:29:49.793Z",
            "location":
            "https://example.com/v2/Users/2819c223-7f76-453a-919d-13861904646",
            "version":"W\/\"f250dd84f0671c3\""
        },
        "emails":[
                {
        "value":"joe.bloggs@example.com"
        }
        ],
        "entitlements": [
                {"value": "eu.
era
        rail.sdi.diagnostic-read"},
                {"value": "eu.
era
        rail.ssi.security-read"}
        ]
        ],
    }
    ]
}
```

[SPPRAMSS-9818 **]**

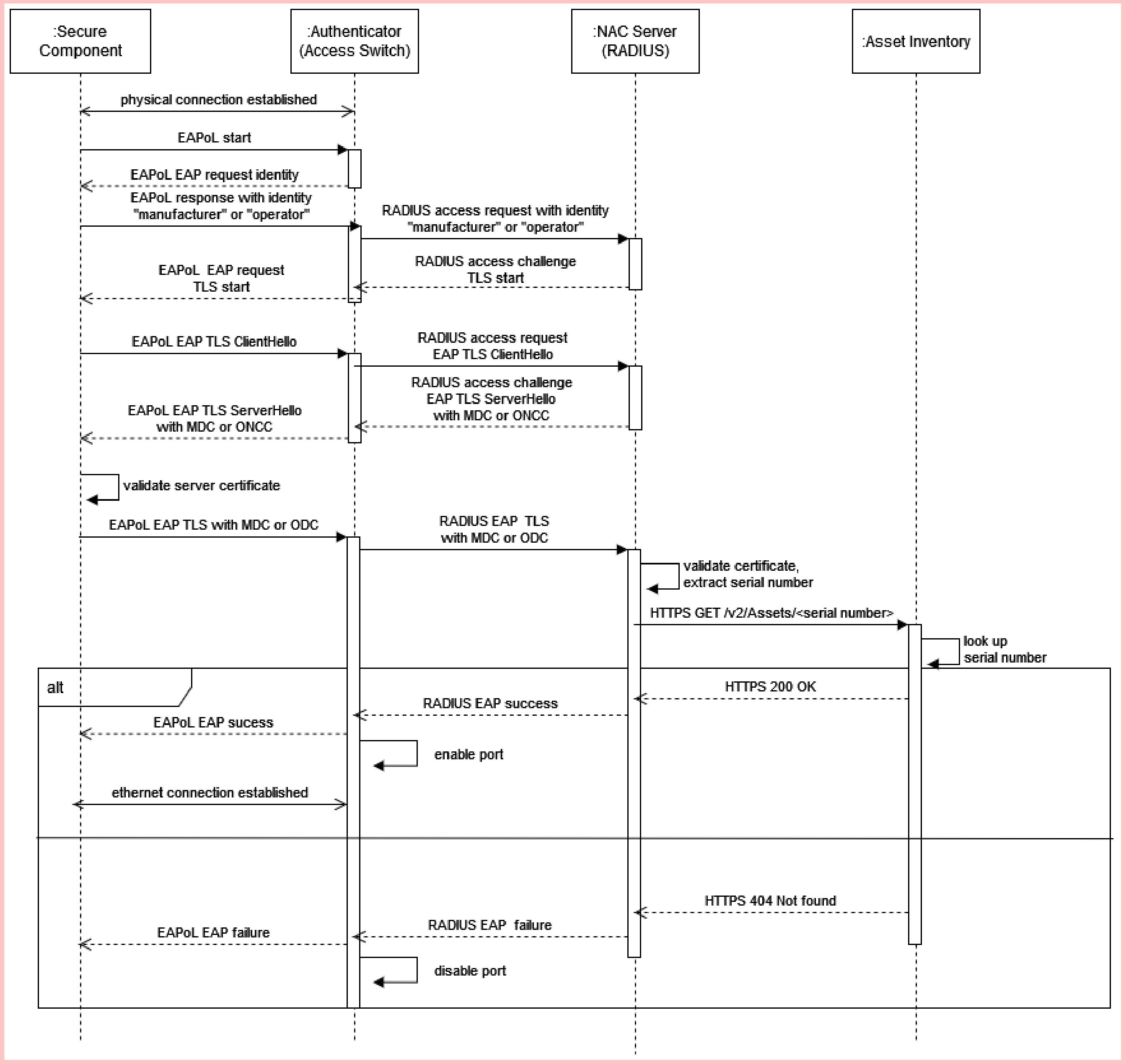
Note2: additional attributes are allowed

, SP-SEC-SERVServ-8-1 - The purpose of the SSI Network Access Control (SSI-NAC) interface is to prevent unauthorized access to the network. The NAC system shall identify, authenticate, and authorize the entity attempting to access the network. IEEE 802.1X is used as basis for the Network Access Control solution. **[**SPPRAMSS-4814 **]**

, SP-SEC-SERV-8-2 - IEEE 802.1X is a standard for network authentication for wired and wireless networks. Amongst other authentication methods, IEEE 802.1X supports the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. EAP-Transport Layer Security (EAP-TLS) allows mutual authentication between a client and a network. The SSI network autentication system consists of four components:

- the supplicant, in this case the Secure Component, is the device attempting to gain access to the network,
- the Network Device, which is the gatekeeper to the network and permits or denies access to the supplicants typically located on network switches,
- the Network Authentication Server providing information required for authentication and informing the Network Device to deny or permit access to the supplicant,
- the Asset Inventory providing information about allowed assets in automation system.

[SPPRAMSS-4815 **]**


:Secure Component
:Authenticator (Access Switch)
:NAC Server (RADIUS)
:Asset Inventory
physical connection established
EAPoL start
EAPoL EAP request identity
EAPoL response with identity "manufacturer" or "operator"
RADIUS access request with identity "manufacturer" or "operator"
EAPoL EAP request TLS start
RADIUS access challenge TLS start
EAPoL EAP TLS ClientHello
RADIUS access request EAP TLS ClientHello
EAPoL EAP TLS ServerHello with MDC or ONCC
RADIUS access challenge EAP TLS ServerHello with MDC or ONCC
validate server certificate
EAPoL EAP TLS with MDC or ODC
RADIUS EAP TLS with MDC or ODC
validate certificate, extract serial number
HTTPS GET /v2/Assets/<serial number>
look up serial number
alt
HTTPS 200 OK
RADIUS EAP success
EAPoL EAP sucess
enable port
ethernet connection established
HTTPS 404 Not found
RADIUS EAP failure
EAPoL EAP failure
disable port

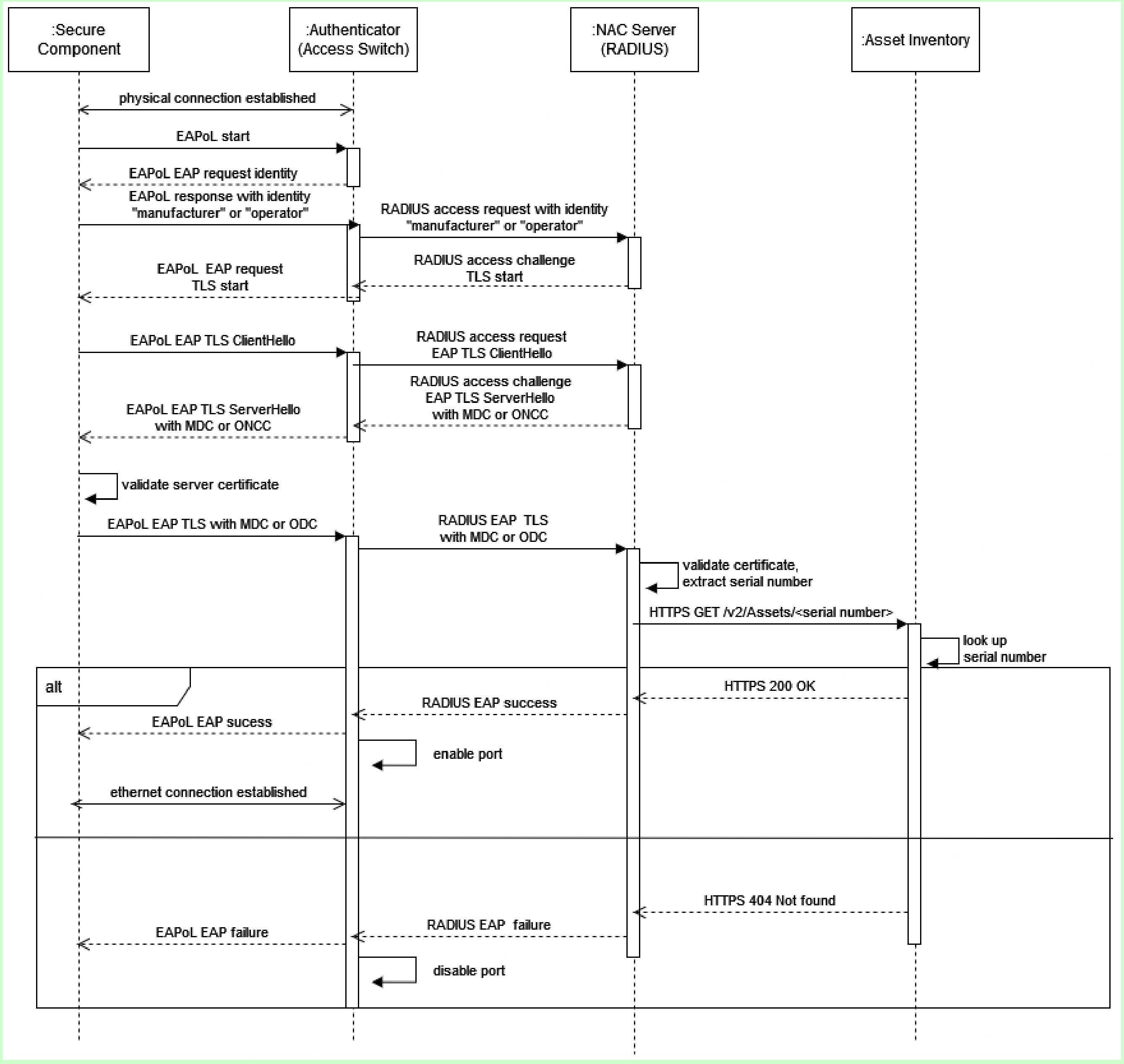

:Secure Component
:Authenticator (Access Switch)
:NAC Server (RADIUS)
:Asset Inventory
physical connection established
EAPoL start
EAPoL EAP request identity
EAPoL response with identity "manufacturer" or "operator"
RADIUS access request with identity "manufacturer" or "operator"
RADIUS access challenge TLS start
EAPoL EAP request TLS start
EAPoL EAP TLS ClientHello
RADIUS access request EAP TLS ClientHello
RADIUS access challenge EAP TLS ServerHello with MDC or ONCC
EAPoL EAP TLS ServerHello with MDC or ONCC
validate server certificate
EAPoL EAP TLS with MDC or ODC
RADIUS EAP TLS with MDC or ODC
validate certificate, extract serial number
HTTPS GET /v2/Assets/<serial number>
look up serial number
alt
HTTPS 200 OK
RADIUS EAP success
EAPoL EAP sucess
enable port
ethernet connection established
HTTPS 404 Not found
RADIUS EAP failure
EAPoL EAP failure
disable port

Figure 8

Figure 6 Network authentication sequence (positive and negative response as alternatives)

, SP-SEC-SERVServ-8-32 - The SSI-NAC interface shall realize network authentication using SP-SEC-Serv-2.3-5 - [IEEE 802.1x1X-2020]. **[**SPPRAMSS-10039 **]**

, SP-SEC-SERVServ-8-43 - The SSI-NAC interface shall realize the EAP-TLS protocol as described in RFC 5216. **[**SPPRAMSS-4817 **]**SP-SEC-Serv-2.3-21 - [RFC 9190].

, SP-SEC-SERVServ-8-54 - The SSI-NAC interface shall realize the RADIUS protocol as described in SP-SEC-Serv-2.3-7 - [RFC 2865]. **[**SPPRAMSS-4862 **]**

, SP-SEC-SERV-8-6 - The SSI-NAC server shall listen on UDP port 1812 for incoming RADIUS requests. **[**SPPRAMSS-4864 **]**

, SP-SEC-SERV-8-7 - The SSI-NAC server shall be configured to use the same shared secret as the Network Device. **[**SPPRAMSS-4888 **]**

, SP-SEC-SERVServ-8-85 - The SSI-NAC server shall reply to RADIUS requests using the Operator Non-safety Communication Certificate (ONCC) MDC or ODC to authenticate itself towards the Secure

Component. [SPPRAMSS-4897]

, **SP-SEC-SERVServ-8-96 -** The SSI-NAC server shall extract the serial number of the MDC of the requesting Secure Component from the MDC (see 6.2.3 - Manufacturer Certificates). **[**SPPRAMSS-4945 **]**SP-SEC-Serv-14.1.1-1).

, **SP-SEC-Serv-8-7 -** The SSI-NAC server shall extract the CN of the ODC of the requesting Secure Component (see SP-SEC-Serv-14.1.2-1).

, **SP-SEC-SERVServ-8-108 -** The SSI-NAC server shall use the SSI-IAM interface to check if the requesting Secure Component's is authorized in the SSI-IAM's Asset Inventory.

Note: A Secure Component is authorized if its serial number (for MDC) or CN (for ODC) exists in the Asset Inventory . **[**SPPRAMSS-4944 **]**and its state is active.

, **SP-SEC-SERVServ-8-119 -** If the Secure Component's serial number exists in the SSI-IAM's Asset Inventory, the Network Authentication Server shall reply with a RADIUS EAP success . **[**SPPRAMSS-4946 **]**to the RADIUS authenticator.

, **SP-SEC-SERVServ-8-1210 -** If the Secure Component's serial number does not exist in the Asset Inventory, the Network Authentication Server shall reply with a RADIUS EAP failure . **[**SPPRAMSS-4947 **]**to the RADIUS authenticator.

SP-SEC-SERVServ-8-1311 - The Requirements for the Authenticator are defined in the Secure Component Specification in chapter Network Access Control Support. **[**Text, SPPRAMSS-4943 **]**Chapter 5.4.3 of SP-SEC-Serv-2.3-27 - [SP-SEC-CompSpec].

, **SP-SEC-SERVServ-9-1 -** The Security Logging Interface enables the transmission of logs from devices via relays to a central service. Logs are used to detect attacks on the system to initiate mitigations. In contrast, Security Diagnostic contains the current state of the Secure Component, based on a diagnostics model. **[**SPPRAMSS-7975 **]**

, **SP-SEC-SERVServ-9-2 -** The Security Logging consists of syslog log originators (which creates log messages), one or more syslog relays (which forwards and potentially filters log messages) and syslog collectors (which analyse the logs).

[SPPRAMSS-4403 **]**

, **SP-SEC-SERVServ-9-3 -** The following Figure depicts an example for a logging architecture. The exact implementation is not defined in this document.

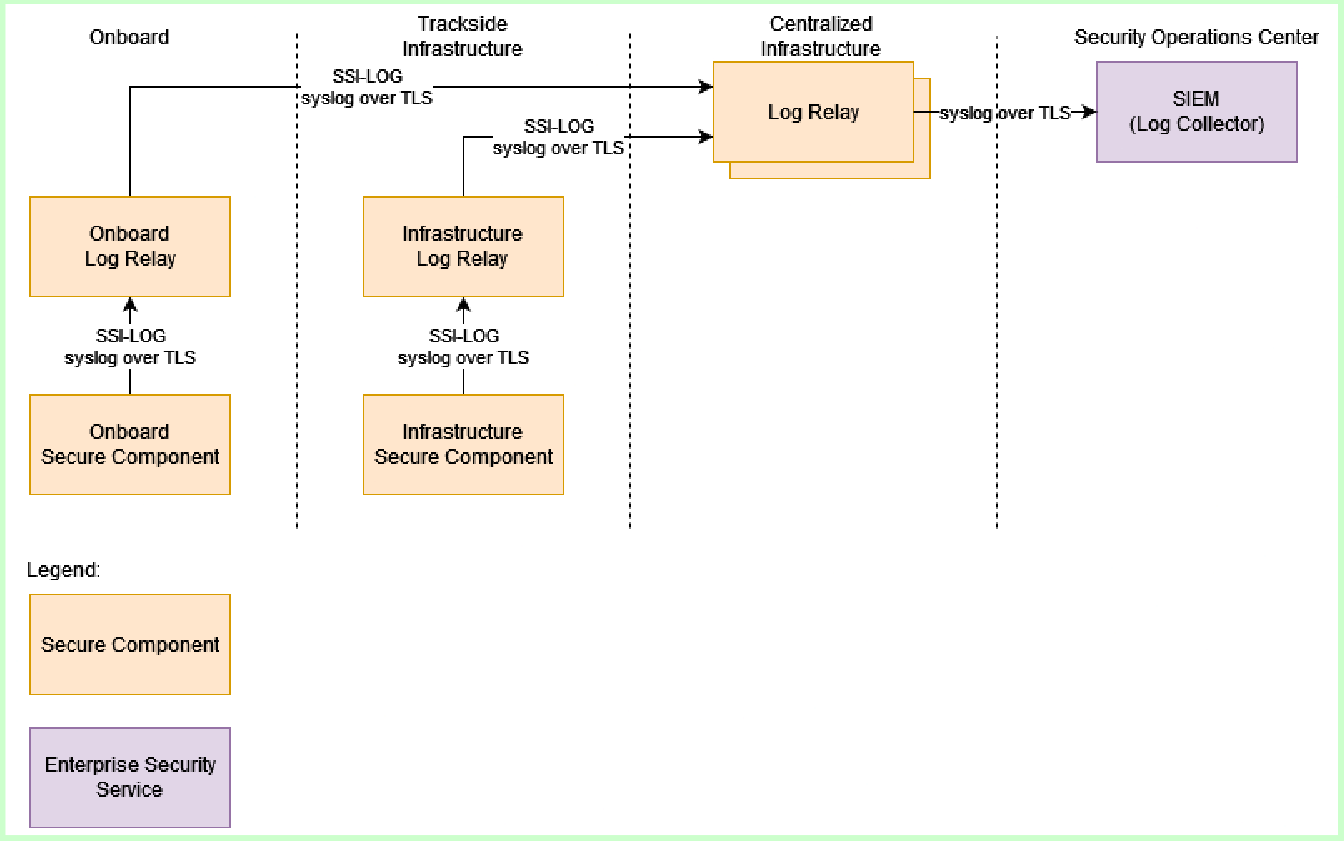


Figure 97 Exemplary Architecture of the Log Services

[SPPRAMSS-4786]

, SP-SEC-SERVServ-9-4 - The Security Logging (LOG) of the Shared Cybersecurity Services is a syslog relay service which collects, potentially filters or correlates and forwards the log messages to upstream log relays or log collectors.

[SPPRAMSS-4402]

, SP-SEC-SERVServ-9-5 - The communication partners using the SSI-LOG (Log Originator, Log Relay, Log CollectorSecure Component, log relay, log collector) shall use syslog over TLS as defined in RFC SP-SEC-Serv-2.3-10 - [RFC 5424] and SP-SEC-Serv-2.3-11 - [RFC 5425] for sending and/or receiving security log messages.

[SPPRAMSS-4404]

, SP-SEC-SERV-9-6 - The Security Logging (Log Relay) shall forward log messages via syslog over TLS as defined in RFC 5424 and RFC 5425. [SPPRAMSS-4408]

, SP-SEC-SERVServ-9-76 - The communication partners using the SSI-LOG (Log Originator, Log Relay, Log CollectorSecure Component, log relay, log collector) shall use for each syslog-over-TLS connection an Operator Non-safety Communication Certificate (ONCC). [SPPRAMSS-4409]

, SP-SEC-Serv-9-7 - For backwards compatibility, legacy components can send security log messages via syslog without TLS. In this case, neither the integrity nor the confidentiality of the log messages are protected.

, SP-SEC-SERVServ-9.1.1-1 - Log messages shall conform to the syslog format as defined in SP-SEC-Serv-2.3-10 - [RFC 5424]. [SPPRAMSS-4795]

, SP-SEC-SERVServ-9.1.1-2 - If a log message is not created by 3rd party software, the log message shall conform to the structured data format of defined in Chapter 6.3 of SP-SEC-Serv-2.3-10 - [RFC 5424 chapter 6].3

Note: This means, that 3rd party software (e.g. open source software) does not need be adapted. [SPPRAMSS-7522]

, SP-SEC-SERVServ-9.1.1-3 - The Log Originator shall set If a log message is not created by 3rd party software, the log message shall contain the SD-ID set to “ERJU_SLOG@” + vendor private enterprise number (see https://www.iana.org/assignments/enterprise-numbers). [SPPRAMSS-4823]SP-SEC-Serv-2.3-2 - [IANA PENs]).

, SP-SEC-SERVServ-9.1.1-4 - If a log message is not created by 3rtd 3rd party software, the log message shall contain the following parameter names in the structured data field: user, credential, action, object, src, status, reason, and contentid. [SPPRAMSS-4807]

Table 6 Log Structured Data fields

Keyword (PARAM-NAME as defined in **RFC5424**[RFC 5424])	**Description**	**Allowed values** (PARAM-**VALUE** VALUE as defined in **RFC5424**[RFC 5424], additional values are allowed)	**Examples**
user	String representing the entity triggering the action, e.g., the user authenticating or causing the change to happen.	• Username/ID • Process-name:PID • Unknown – if the entity is not identified • None – if no user is associated with this action e.g., resource exhaustion	John_Doe1 (human user) 820xauth:34593 (SW process)
credential	String representing the type of credentials used to perform the associated action, e.g., the user authenticating or changing.	• X509cert – certificate-based authentication • SSHcert – certificate-based authentication (ssh only) • pwAuth – password-based authentication • IAMSSOtoken – Bearer token-based authentication • local – for local access without explicit authentication	X509cert SSHcert pwAuth IAMSSOtoken local

Keyword (PARAM-NAME as defined in **RFC5424**[RFC 5424])	**Description**	**Allowed values** (PARAM-**VALUE** VALUE as defined in **RFC5424**[RFC 5424], additional values are allowed)	**Examples**
action	Human-readable free text in English describing, what happened.	Human-readable free text in English, however, starting with a keyword is recommended, which identifies the broad action type.	login access change monitor
object	String describing, what was affected by the performed action, e.g., a session created, malicious file opened, rasta connection disturbed, ….	• Component name/id • Account • File name • Data resource name • Process-name:PID	OPC.UA.Model.ModuleX John_Doe1 (human user) /etc/conf.xml sda3
src	String representing the source of the event.	• IP address:Port number – for remotely triggered events • Process name:PID – local events • FQDN • EULYNX technical identifier	10.10.1.20:1043 [fe80:1111::4444:0:0]:8888 webserver:4951 localhost **ETCS FQDN example:** Id8470f.ty01.etcs **EULYNX technical identifier example:** [country code][area designator][system type][code][tag][sequence no] DEHG2_XIO___37##0005
status	String description of the action status.	• Success • Failure • Unknown • Empty String (e.g., for availability events)	success failure unknown

Keyword (PARAM-NAME as defined in **RFC5424**[RFC 5424])	**Description**	**Allowed values** (PARAM-**VALUE** VALUE as defined in **RFC5424**[RFC 5424], additional values are allowed)	**Examples**
reason	Human-readable free text in English demonstrating the reason and the way of action.	Human-readable free text in English	“invalid chain of trust: root XYZ not accepted”
contentid	String defining a unique message ID for translation purposes	A unique ID for this log message (see naming scheme below)	SSI_IAM_OPC_UA_MSG_13

, SP-SEC-Serv-9.1.1-5 - A log message can optionally contain the following parameter names in the structured data field: serial

Keyword (PARAM-NAME as defined in [RFC 5424])	**Description**	**Allowed values** (PARAM-VALUE as defined in [RFC 5424], additional values are allowed)	**Examples**
serial	Manufacturer serial number of the device sending the log message	Free text	12345679-01

, SP-SEC-SERVServ-9.1.2-1 - The following requirements are applicable for custom-made software. These requirements are not mandatory for 3rd party software. **[**SPPRAMSS-9607 **]**

, SP-SEC-SERVServ-9.1.2-2 - The log originator shall set the facility of the syslog header to 4 (security/authorization messages) as defined in SP-SEC-Serv-2.3-10 - [RFC 5424]. **[**SPPRAMSS-7976 **]**

, SP-SEC-SERVServ-9.1.2-3 - The Log Originator log originator shall set the SEVERITY of the syslog header for debug messages for application developers to "7" (debug). **[**SPPRAMSS-4805 **]**

, SP-SEC-SERVServ-9.1.2-4 - The Log Originator log originator shall set the SEVERITY of the syslog header for the audit log to "6" (info) in case of a successful event (e.g. successful authentication) to "6" (info). **[**SPPRAMSS-4806 **]**

, SP-SEC-SERVServ-9.1.2-5 - The Log log originator shall set the SEVERITY of the syslog header for the audit log to "4" (warning) in case of an unsuccessful event (e.g. unsuccessful authentication, unsuccesful threat) to "4" (warning). **[**SPPRAMSS-4804 **]**

, **SP-SEC-SERVServ-9.1.2-6 -** The Log log originator shall set the SEVERITY of the syslog header for all error conditions not requiring immediate action, but human attention to "3" (error). **[**SPPRAMSS-4810 **]**

, **SP-SEC-SERVServ-9.1.2-7 -** The Log log originator shall set the SEVERITY of the syslog header for all events requiring immediate action, likely by a human, to "1" (alert). **[**SPPRAMSS-4811 **]**

SP-SEC-SERVServ-9.1.2-8 - The following table gives examples for the use of severity levels:
Note: Debug messages are not included in this table because they are highly application-specific.

Table 7 Examples of syslog structured data

Log Type	6 – Info	4 – Warning	3 – Error	1 – alert
AAA (Authentication, Authorization, Access)	Successful authentication or authorization decisions Successful remote access, including from one application component to another in a distributed environment Significant system access, data access, and application component access	Failed authentication or authorization decisions Failed remote access attempts	Repetitive failed authentication resulted in a locked user account	
Change	Successful changes, e.g: System or application changes (especially privilege changes) Data changes (including creation and destruction) Application and component installation and changes Changes to PKI (certificate requests, certificate revocations)	Unsuccessful changes CRL update failure	System changes could affect security and availability	System changes lead to a security and availability problems Changes of security configuration Factory reset

Log Type	6 – Info	4 – Warning	3 – Error	1 – alert
Threat		Attack attempts and probes (e.g. pings, nmap scans, connection attempsattempts, to unsued unused ports)	Attacks that have a high chance of being successful (e.g. malformed requests)	Attacks that are successful (e.g. unexpected states within application, failed runtime integrity checks in process whitelisting / security configuration)
Resource	Statistical resource information	System reaching or falls below a first water mark value (warning level threshold)	System reaching a high water mark value, system operation might be endangered in some time System falls below high water mark value. Faults that can affect a system operation	System reaching capacity, system operation is endangered System recovers from capacity errors
Availability	Status messages of hardware, systems, applications or components	Startup/shutdown/restart of systems, applications or components	Failures of systems, applications or components	Crashes of systems, applications or components

[Text, SPPRAMSS-4803]

, **SP-SEC-SERVServ-9.1.2-9 -** The timestamp of the syslog header contains the time when the log message was created on the originating system (syslog originator). [SPPRAMSS-4826]

, **SP-SEC-SERVServ-9.1.2-10 -** The Log originator shall set the timestamp of the syslog header to the current time as defined in /SP-SEC-Serv-2.3-10 - [RFC 5424/ using] using UTC date/time format including milliseconds using TIME-SECFRAC.

Note: Example: 2023-09-14T:14:15:30.003Z [SPPRAMSS-4819]An Example for for such a timestamp is `2038-01-19T:03:14:08.000Z`

, **SP-SEC-SERV-9.1.2-11 -** HOSTNAME contains an Identifier for the machine that sent the log message. [SPPRAMSS-4829]

, **SP-SEC-SERVServ-9.1.2-1211 -** The LOG originator shall set the HOSTNAME to one of the following values: FQDN, static IP address, hostname or , dynamic IP address . [SPPRAMSS-4831] or use-case specific identifier (e.g. etcs FQDN with board number as suffix).

Note: HOSTNAME contains an Identifier for the machine that sent the log message

, **SP-SEC-SERVServ-9.1.2-1312 -** The APP-NAME is a String containing the identification of the application that created the log message. **[**SPPRAMSS-4836 **]**

, **SP-SEC-SERVServ-9.1.2-1413 -** Process ID of the syslog daemon is automatically set by syslog implementation. **[**SPPRAMSS-4834 **]**

, **SP-SEC-SERVServ-9.1.2-1514 -** The LOG Orginator Originator shall set the MSGID as defined in SP-SEC-Serv-2.3-10 - [RFC 5424] to one of the following values:

- AAA (Authentication, Authorization, Access)
- Change
- Threat
- Resource
- Availability
- Debug
- Others

[SPPRAMSS-4838 **]**

- Other

, **SP-SEC-SERVServ-9.1.2-1615 -** The msg part of the syslog message is optional if the structured data contains all necessary information. **[**SPPRAMSS-4844 **]**

, **SP-SEC-SERVServ-9.1.2-1716 -** If the msg part is used, the LOG originator shall use UNICODE with UTF-8 encoding. **[**SPPRAMSS-4843 **]**

, **SP-SEC-SERVServ-9.1.2-1817 -** If the msg part is used, the LOG originator shall not use Octet values below 32 (control character range). **[**SPPRAMSS-4846 **]**

SP-SEC-SERVServ-9.2-1 - These examples showcase how log messages are structured:

- Authentication failure due to untrusted root certificate
  ```
  <syslog header>[ERJU_SLOG@32473 user="John_Doe1" credential=”X509cert”
  action=”login” object=”OPC.UA.Model.ModuleX” src=”10.10.1.20:1043”
  status=”failure” reason=”invalid chain of trust: root XYZ not trusted”
  contentid=”SSI_IAM_OPC_UA_MSG_13”]
  ```
- Process whitelisting runtime integrity check failed
  ```
  <syslog header>[ERJU_SLOG@32473 user="whitelistingruntime-integrity-
  daemon:5" credential=”local” action=”monitor” object=”/usr/bin/openssl”
  src=”localhost” status=”failure” reason=”Integrity check failed for binary
  /usr/bin/openssl” contentid=”SECCOMP_PROCESS_
  WHITELISTINGRUNTIME_INTEGRITY_MSG_1”]
  ```
- Secure Component Sending a Certificate Request
  ```
  <syslog header>[ERJU_SLOG@32473 user="certificate-maintainer:6"
  credential=”local” action=”change” object=”new operator device certificate”
  src=”localhost” status=”success” reason=”Send certificate request for new
  ```

```
    operator device certificate” contentid=”SECCOMP_CERT_MAINTAINER_MSG_3”]
```

[Text, SPPRAMSS-4860]

, SP-SEC-Serv-10-1 - The User Authentication Service enables authentication of human users.

Note: User authentication on operating system level is not part of this standard.

, SP-SEC-SERVServ-10-12 - The SSI-UAS shall support multi-factor authentication of human users. [SPPRAMSS-4675]

, SP-SEC-SERVServ-10-23 - The SSI-UAS shall implement single sign-on (SSO) based on OpenID Connect 1.0 (OIDC) as defined in https://openid.net/specs/openid-connect-core-1_0.html [SPPRAMSS-6055]in SP-SEC-Serv-2.3-4 - [OIDC 1.0].

, SP-SEC-SERVServ-10-34 - The SSI-UAS shall use the "OAuth 2.0 Authorization Code Flow " as defined in SP-SEC-Serv-2.3-4 - [OIDC 1.0] when authenticating human users.

NoteNote1: This means, that ID Tokens, Authorization Codes and Access Tokens need to be handled by the client. This functionality is supported by browsers and HTTP libraries such as wget and curl. [SPPRAMSS-6066]

Note2: The use of PKCE as defined in SP-SEC-Serv-2.3-13 - [RFC 7636] is recommended.

, SP-SEC-SERVServ-10-45 - The SSI-UAS shall support authentication with X.509 client certificates complying to the Operator Human User Certificate (OHUC) profile . [SPPRAMSS-6575]see SP-SEC-Serv-14.1.2-4.

, SP-SEC-SERVServ-10-56 - The SSI-UAS shall support authentication with username/password with at least one additional factor (e.g. authenticator apps using TOTP (time-based one-time-password)). [SPPRAMSS-6574]

, SP-SEC-SERVServ-10-67 - The SSI-UAS should support passwordless authentication with at least one additional factor (e.g. passkeys with biometric factor). [SPPRAMSS-6576]

, SP-SEC-SERVServ-10.1-1 - For Access Tokens, the SSI-IAM shall use at least the JWT claims defined as mandatory for Access Tokens in SPPRAMSS-6578.

[SPPRAMSS-6068]in SP-SEC-Serv-10.1-3 - JWT claims for Access Tokens and ID Tokens.

, SP-SEC-SERVServ-10.1-2 - For ID tokens, the SSI-IAM shall use at least the JWT claims defined as mandatory for ID tokens in SPPRAMSS-6578. [SPPRAMSS-6559]SP-SEC-Serv-10.1-3.

, SP-SEC-SERVServ-10.1-3 - JWT claims for Access Tokens and ID Tokens [SPPRAMSS-6578]

Claim	Description	Use in JWT access token	Use in JWT ID token
sub	Subject identifier of the user that requested the token.	mandatory	mandatory
iss	Issuer of the token.	mandatory	mandatory
aud	Identifier of the audience the token is intended for. Shall be set to the URL of the service to be accessed.	mandatory	mandatory

Claim	Description	Use in JWT access token	Use in JWT ID token
exp	Expiration time of the token. The lifetime should not be longer than the maximum session idle time at the service to be accessed (e.g. 30 minutes).	mandatory	mandatory
jti	JWT ID. Unique identifier of the token. Automatically generated by the OpenID Provider.	mandatory	mandatory
scope	Scope values for authorization. Shall only contain the permissions of the user.	mandatory	no
auth_time	Time of user authentication.	recommended	recommended
nonce	Value used to associate a Client session with an ID Token.	recommended	recommended
amr	Authentication Method Reference. Allowed values as defined in SP-SEC-Serv-2.3-17 - [RFC 8176] • sc and pin • pwd and mfa and otp • (hwk or swk) and (fpt or face)	mandatory	mandatory
email	email address of the authenticated user.	mandatory	mandatory

Claim	Description	Use in JWT access token	Use in JWT ID token
sub	Subject identifier of the user that requested the token.	mandatory	mandatory
iss	Issuer of the token.	mandatory	mandatory
aud	Identifier of the audience the token is intended for. Shall be set to the URL of the service to be accessed.	mandatory	mandatory
exp	Expiration time of the token. The lifetime should not be longer than the maximum session idletime at the service to be accessed (e.g. 30 minutes).	mandatory	mandatory
jti	JWT ID. Unique identifier of the token. Automatically generated by the OpenID Provider.	mandatory	mandatory
scope	Scope values for authorization. Shall only contain the permissions of the user.	mandatory	no
auth_time	Time of user authentication.	recommended	recommended
nonce	Value used to associate a Client session with an ID Token.	recommended	recommended

Claim	Description	Use in JWT access token	Use in JWT ID token
amr	Authentication Method Reference. Allowed values according to https://datatracker.ietf.org/doc/html/rfc8176#section-2 : • sc and pin • pwd and mfa and otp • (hwk or swf) and (fpt or face)	mandatory	mandatory
email	email address of the authenticated user.	mandatory	mandatory

, SP-SEC-SERVServ-10.1-4 - The SSI-IAM shall set the validity time of the access token to a configurable maximum time.

Note: The maximum validity of the access token is set to be in line with the security policies of the Infrastructure Manager and the practical feasibility in daily operation. **[**SPPRAMSS-6671 **]**

, SP-SEC-SERVServ-10.2-1 - If the SSI-UAS server receives an ID or access token, the SSI-UAS server shall verify the token signature before accepting it. **[**SPPRAMSS-6563 **]**

, SP-SEC-SERVServ-10.2-2 - If the SSI-UAS server receives an ID or access token, the SSI-UAS server shall verify that all mandatory token claims as defined in SP-SEC-SERVServ-10.1-3 - JWT claims for Access Tokens and ID Tokens are included in the token. **[**SPPRAMSS-6580 **]**

, SP-SEC-SERVServ-10.2-3 - If the SSI-UAS server receives an ID or access token, the SSI-UAS server shall verify the content of all mandatory token claims as defined in SP-SEC-SERVServ-10.1-3 - JWT claims for Access Tokens and ID Tokens **[**SPPRAMSS-6583 **]**

, SP-SEC-SERVServ-10.2-4 - If the SSI-UAS server receives an ID or access token with a recommended claim according to SP-SEC-SERVServ-10.1-3 - JWT claims for Access Tokens and ID Tokens, the SSI-UAS shall verify the content of the recommended token claims. **[**SPPRAMSS-6581 **]**

, SP-SEC-SERVServ-11-1 - Backups are intended for operational data that is relevant for operational availability (e.g. changes in databases), but is not part of the configuration (e.g. obtained via SMI). Most rail automation devices receive all data required for operational data via SMI and do not need the interface SSI-BKP. For the Shared Cybersecurity Services, the following services require backups:

- **IAM** - Identity and Access Management
- **UAS -** User Authentication Service

Other services that require backups are:

- **MDM** - Maintenance and Data Management: makes configuration and software available to devices.

[Text, SPPRAMSS-9700 **]**

- Note: MDM is defined in EULYNX Eu.Doc.18

, **SP-SEC-SERVServ-11-2 -** A backup creation can be triggered from a central service management station. The central service management station may be landside and/or onboard. This backup is transferred via HTTPS POST to a URI defined by the input parameter of the OPC UA call. **[**SPPRAMSS-4483 **]**

, **SP-SEC-SERVServ-11-3 -** Backup creation can be triggered locally by a Secure Component. This backup is transferred via HTTPS POST to a preconfigured default URI. **[**SPPRAMSS-4538 **]**

, **SP-SEC-SERVServ-11-4 -** A backup shall consist of two files:

- `<YYYYMMDDThhmmssZ>_<secure-component-type>_<application-id>.tar.gz`: the component-specific backup artifact as gzipped tar archive (.tar.gz) as defined in RFC 1950SP-SEC-Serv-2.3-6 - [RFC 1952]
- `<YYYYMMDDThhmmssZ>_<secure-component-type>_<application-id>.metadata.json:` containing the backup metadata.

[SPPRAMSS-4486 **]**

, **SP-SEC-SERVServ-11-5 -** The SSI-BKP interface shall implement the following OPC UA methods:

Table 8 OPC UA methods for SSI-BKP

Method Name	Description	Input Arguments	Output Arguments
`CreateBackup`	Trigger backup creation from central service	URL: prefix of the URL for upload of the backup humanReadableTag: user supplied tag that is inserted into the Metadata File for easier identification of the backup machineReadableTag: user supplied tag that is inserted into the Metadata File for easier identification of the backup encryptCert: optional certificate (and trust chain) in PEM format that will be used to derive a key for encryption of the Backup Archive	Success (use status variables for more info), Failure (status variables are irrelevant)

Method Name	Description	Input Arguments	Output Arguments
`RestoreBackup`	Trigger restoration of backup from central service	URL: prefix of the URL for download of the backup	Success (use status variables for more info), Failure (status variables are irrelevant)

[SPPRAMSS-4539] Note: these methods are provided by the OPC UA server running on the device which requires backup.

, SP-SEC-SERVServ-11-6 - The SSI-BKP interface shall implement at least provide the the following OPC UA variables for report status variablesinformation:

Table 9 OPC UA variables for SSI-BKP

Variable Name	Variable Type	Possible values	Description
BackupCreationStatus	String	100 - Idle 200 - Creating 201 - Failure during creation 500 - Uploading 501 - Failure during upload 900 - TransferCompleted -1 - unexpected error	
BackupRestorationStatus	String	100 - Idle 200 - Downloading 201 - Failure during download 500 - Restoring 501 - Failure during restoring 900 - TransferCompleted -1 - unexpected error	

Note: Note1: these variables are provided by the OPC UA server running on the device which requires backup.

Note2: more detailed failure states can be implemented using values not defined in this table. [SPPRAMSS-4541]

, SP-SEC-Serv-12-1 - The following security maintenance method and diagnostic value definitions should be implemented using the protocols defined in SDI.

, SP-SEC-Serv-12.1-1 - The SSI-MNT interface shall provide the diagnostic value Security:SecurityStatus (Boolean) to represent the overall security status of the component.

Note: the value is TRUE when no security related issues (expired certificates, integrity errors, availibility errors to SSI, are currently present, , the value is FALSE when security issues are currently present.

, SP-SEC-Serv-12.1-2 - The SSI-MNT interface shall provide the diagnostic value Security:IntegrityCheckStatus (Boolean) to represent the status of the integrity checks.

Note: the value is TRUE when no integrity failures have been reported (process allowlist checks, signature checks for files,...) and FALSE when integrity errors have occurred since boot time. Details of errors is available from the security logs.

, **SP-SEC-Serv-12.2-1 -** The SSI-MNT interface shall provide the maintenance method Security:UpdateRevocationsLists() to request the update of the CRLs.

Note: if a CRL update contains a revoked certificate used in current communication, the communication has to be terminated (see SP-SEC-Comp-5.5.2-12).

, **SP-SEC-Serv-12.2-2 -** The SSI-MNT interface shall provide the maintenance method Security:RenewCert(String certID) to renew its certificates.

Note 1: The default method for certificate renewal is done automatically via SSI-PKI interface automatically. The diagnostic method covers edge cases when certificate renewal is necessary before certificate expiration.
Note 2: If the renewed certificate is used in current communication, the communication has to be re-established (see SP-SEC-Comp-5.5.2-6).

, **SP-SEC-Serv-12.2-3 -** The SSI-MNT interface shall provide the maintenance method Security:GetInstalledCerts() (File/String) to obtain the public certificates available on the Secure Component as String / GZIP file as defined in SP-SEC-Serv-2.3-6 - [RFC 1952].
Note: the return value is a compressed file containing all public certificates available on the Secure Component in GZIP file format.

, **SP-SEC-Serv-12.2-4 -** The SSI-MNT interface shall provide the maintenance method Security:GetInstalledTrustAnchors() (String) to obtain a list of installed trusted certificates (trust root / intermediate certificates).
Note: the return value is a compressed file containing the installed and trusted certificates (trust anchors / root certificates).

, **SP-SEC-Serv-12.2-5 -** The SSI-MNT interface shall provide the maintenance method Security:GetInstalledCRLs() () to obtain the list of installed CRLs.

, **SP-SEC-Serv-12.3-1 -** The SSI-MNT interface shall provide the maintenance method Security:GetSecurityLog(Time start, Time end) to access audit logs on a read-only basis for authorised humans and/or software processes.
Note: The default method for log transmission is via SSI-LOG. This diagnostic method covers edge cases when log transmission was interrupted to retrieve local stored logs.

, **SP-SEC-Serv-12.3-2 -** The SSI-MNT interface shall provide the diagnostic value Security:LogSize (Uint64) to represent the size of the log in bytes.

, **SP-SEC-Serv-12.4-1 -** The SSI-MNT interface shall provide the maintenance method Security:GetComponentConfiguration() (String) to return the list of configuration identifiers with corresponding SHA-512 hashes.

Note 1: this maintenance method returns a comma separated list of configurations identifiers with the corresponding SHA-512 hash. Component identifiers and hashes are separated by the character '#".
Note 2: this maintenance method can be used to detect changes in component configuration by comparing the result with previously stored configurations (or hashes).

, **SP-SEC-Serv-12.4-2 -** The SSI-MNT interface shall provide the maintenance method Security:GetNetworkConfiguration() (String) to allow the network configuration properties being retrieved.

Note: this diagnostic method can be used to detect changes in network configuration by comparing the result with previously stored configurations (or hashes).

, **SP-SEC-Serv-12.5-1 -** The SSI-MNT interface shall provide the maintenance method Security:FactoryReset() to purge persistent data to reset the component to factory state.
Note 1: this method can be used as part of a decommissioning process SP-SEC-PGM 10.2 Decommissioning
Note 2: this method does not purge the factory key material (e.g. the MDC together with its root certificates will stay on the devices.
Note 3: this provides the user with the ability to erase data which requires confidentiality from persistent memory.

, SP-SEC-Serv-12.6-1 - The SSI-MNT interface shall provide the maintenance method Security:TestProcessIntegrityCheck() to test the functionality of the process integrity check.

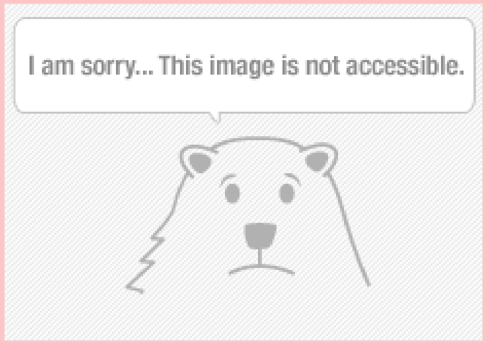
Note: a typical implementation is to have an executable file with no functionality not in part of the process integrity check (e.g. an allowlist). This executable is sill integrity protected, e.g. by secure boot. The executable is executed by this maintenance method. This triggers the process integrity check and issues a log message, which can be used to verify the security functionality of process allowlisting, security logs, time synchronization and real-time clock (time is part of a log message).

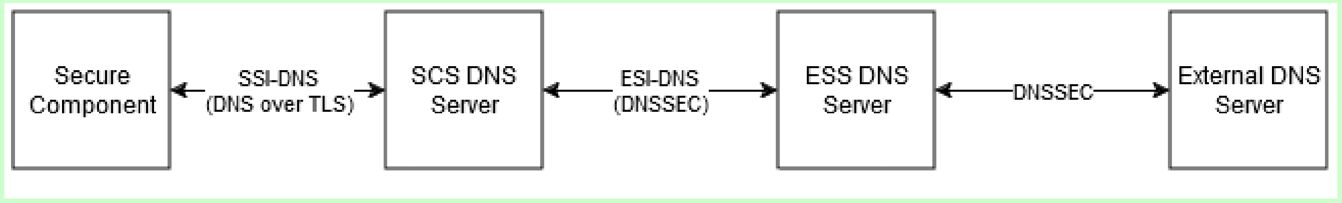
, SP-SEC-Serv-12.6-2 - The SSI-MNT interface shall provide the maintenance method Security:TestHostFirewall() to test the functionality of the host-based firewall.

Note: a typical implementation is to have a process with tries to open a connection when this maintenance method is called to a destination and port which is not in the firewall allowlist . This triggers a block of the firewall and issues a log message, which can be used to verify the security functionality of the host-based firewall.

, SP-SEC-SERVServ-1213-1 - This chapter contains security requirements for Domain Name System (DNS). These requirements are applicable when DNS is used. The architectural decisions regarding DNS are out of scope of the security domain. DNS consists of two interfaces:

- ESI-DNS: between DNS servers (transfer and validation of zone contents)
- SSI-DNS: between DNS client and DNS server (DNS lookups)





Secure Components use DNS over TLS for DNS lookups. To reduce complexity, DNSSEC is not used by Secure Components.

DNS servers ensure integrity Integrity of DNS records provided by ESS DNS servers or external DNS servers is ensured by using DNSSEC.
[SPPRAMSS-6652]

, SP-SEC-SERV-12-2 - If DNS is used, the ESS-DNS server shall provide authenticated DNS records using the DNS Security Extensions (commonly called DNSSEC) as defined in RFC 9364. **[SPPRAMSS-5691]**

, SP-SEC-SERVServ-1213-32 - If DNS is used, a It is recommended that the SCS DNS server shall validate validates the DNS records provided by the higher DNS server using DNSSEC as defined inSP-SEC-Serv-2.3-22 - [RFC 9364]. **[SPPRAMSS-8157]**

, SP-SEC-SERVServ-1213-43 - If DNS is used, the The SSI-DNS server shall use DNS over TLS as defined in in SP-SEC-Serv-2.3-16 - [RFC 7858]. **[SPPRAMSS-5690]**

, **SP-SEC-SERVServ-1213-54 -** If DNS is used, the The SSI-DNS server shall use an Operator Non-Safety Communication Certificates (ONCC) for DNS over TLS. **[SPPRAMSS-5693]**

, **SP-SEC-SERVServ-1213-65 -** If DNS is used, the The SSI-DNS client shall use DNS over TLS as defined inSP-SEC-Serv-2.3-16 - [RFC 7858]. **[SPPRAMSS-8158]**

, **SP-SEC-SERVServ-1314.1.1-1 -** MDC

Table 10 Manufacturer Device Certificate (MDC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[expected lifetime of the device after creation date]	recommended validity is at least 30 years

Subject	**mandatory:**
	CN=[product name]
	serialNumber=[manufacturer-unique device serial number]
	recommended:
	O=[manufacturer name]
	C=[manufacturer country]
		Additional manufacturer-specific attributes are allowed.

Subject Public Key Info	[public key], secp521r1	
X.509 v3 Extensions		
Authority Key Identifier	[key identifier of issuers public key]	
Subject Key Identifier	[key identifier of own public key]	
Key Usage (critical)	**mandatory:** digitalSignature keyAgreement	Additional key usages are allowed to enable additional use cases.
Subject Alternative Name	[manufacturer-specific, e.g. OID structure]	Optional
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to RFC 5280 SP-SEC-Serv-2.3-9 - [RFC 5280]

Field Name	Content	Comment
CRL Distribution Points	**optional:** [manufacturer-specific distributionPoint]	optional, if used, the Secure Components download CRLs from the URL

[SPPRAMSS-7641]

, SP-SEC-SERVServ-1314.1.1-2 - MCSC

Table 11 Manufacturer Config Signer Certificate (MCSC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of MSICAC]	
Validity	[manufacturer-specific period]	recommended validity period is 1 year

Subject	**mandatory:**
	CN=[unique manufacturer-specific CN]
	recommended:
	OU=[manufacturer-specific organization]
	C=[manufacturer-specific country]
		Additional manufacturer-specific attributes are allowed.

Subject Public Key Info	[public key], secp521r1	
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	
Extended Key Usage (critical)	id-kp-configSigning	OID: 1.3.6.1.45.15.43297.443.1.141
Subject Alternative Name	[manufacturer-specific]	optional
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to RFC 5280 SP-SEC-Serv-2.3-9 - [RFC 5280]

[SPPRAMSS-7642]

, SP-SEC-SERVServ-1314.1.1-3 - MTASC

Table 12 Manufacturer Trust Anchor Signer Certificate (MTASC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of MSICAC]	
Validity	[manufacturer-specific period]	recommended validity period is 1 year

Subject	**mandatory:**
	CN=[unique manufacturer-specific CN]
	recommended:
	OU=[manufacturer-specific organization]
	C=[manufacturer-specific country]
		Additional manufacturer-specific attributes are allowed.

Subject Public Key Info	[public key], secp521r1	
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	
Extended Key Usage (critical)	trustanchorSigningid-kp-trustAnchorConfigSigning	OID: 1.3.6.1.45.15.43297.443.1.242
Subject Alternative Name	[manufacturer-specific]	optional
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to RFC 5280 SP-SEC-Serv-2.3-9 - [RFC 5280]

[SPPRAMSS-7643]

, SP-SEC-SERVServ-1314.1.1-4 - MUSC

Table 13 Manufacturer Update Signer Certificate (MUSC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	

Field Name	Content	Comment
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of MSICAC]	
Validity	[manufacturer-specific period]	recommended validity period is 1 year

Subject	**mandatory:**
	CN=[unique manufacturer-specific CN]
	recommended:
	OU=[manufacturer-specific organization]
	C=[manufacturer-specific country]
		Additional manufacturer-specific attributes are allowed.

Subject Public Key Info	[public key], secp521r1	
X.509 v3 Extensions		
Authority Key Identifier	[key identifier of issuer public key]	
Subject Key Identifier	[key identifier of owner public key]	
Key Usage (critical)	digitalSignature	
Extended Key Usage (critical)	updateSigningid-kp-updatePackageSigning	OID: 1.3.6.1.45.15.4329 7.443.1.343
Subject Alternative Name	[manufacturer-specific]	optional
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to RFC 5280 SP-SEC-Serv-2.3-9 - [RFC 5280]

[SPPRAMSS-7644]

, SP-SEC-SERVServ-1314.1.2-1 - ODC

Table 14 Operator Device Certificate (ODC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[operator-specific period]	recommended validity period is 1 year

Field Name	Content	Comment

Subject	**mandatory:**
	CN=[operator-specific device identifier]
	serialNumber=[device serial number]
	recommended:
	O=[operator-specific organization]
	C=[operator-specific country]
		Operator-specific device identifier may include the EULYNX technical identifier
		Additional operator-specific attributes are allowed

Subject Public Key Info	[public key], secp521r1	
X.509 v3 Extensions		
Authority Key Identifier	[key identifier of issuer public key]	
Subject Key Identifier	[key identifier of owner public key]	
Key Usage (critical)	**mandatory:** digitalSignature keyAgreement	Additional key usages are allowed to enable additional use cases.
Subject Alternative Name	[operator-specific, e.g. OID structure]	optional
Certificate Policies	[manufactureroperator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-9 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific distributionPoint]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7648]

, SP-SEC-SERVServ-1314.1.2-2 - ONCC

Table 15 Operator Non-Safety Communication Certificate (ONCC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA256withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[operator-specific period depending on purpose]	should be configurable based on operational environmentbased purpose. Recommended validity period is 2 years

Field Name	Content	Comment

Subject	**mandatory:**
	CN=[use-case specific device process identifier]
	serialNumber=[use-case specific]
	recommended:
	O=[operator-specific organization]
	C=[operator-specific country]
	OU=[element abbreviation]
		ETCS use case:
		CN shall be an FQDN as defined in [Subset-037-1].
		serialNumber shall be the ETCS ID as defined in [Subset-146].
		OU shall be the ETCS ID type defined in [Subset-037-1].
		other use cases:
		CN shall be unique, using the technical identifier defined in EULYNX EU.Doc.16.Req Eu.SAS.77
		Additional operator-specific attributes are allowed.

Subject Public Key Info	[public key], secp521r1	
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)	**recommendedmandatory:** digitalSignature keyAgreement **mandatory for OPC UA:** nonRepudiation keyEncipherment dataEncipherment	Additional key usages are allowed to enable additional use cases.
Extended Key Usage	**optional:** serverAuth, clientAuth	serverAuth and/or clientAuth depending of the use case of the certificate

Subject Alternative Name	dNSName=[FQDN]
	iPAddress=[IP address]
	URI=[application URI]
		either dNSName or iPAddress shall be used
		
		for OPC UA, URI shall be used additionally
		Example: urn:hostname:namespace:applicationName

Certificate Policies	[manufactureroperator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-9 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific distributionPoint]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7649]

, SP-SEC-SERVServ-1314.1.2-3 - OSCC

Table 16 Operator Safety Communication Certificate (OSCC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA256withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[operator-specific period depending on purpose]	should be configurable based on operational environment. Recommended validity period is 2 years

Subject	**mandatory:**
	CN=[use-case specific device process identifier]
	serialNumber=[device serial number]
	recommended:
	O=[operator-specific organization]
	C=[operator-specific country]
		ETCS use case:
		CN shall be an FQDN as defined in [Subset-037-1].
		serialNumber shall be the ETCS ID as defined in [Subset-146].
		OU shall be the ETCS ID type defined in [Subset-037-1].
		other EULYNX use casescase:
		CN shall be unique, using the technical identifier defined in EULYNX EU.Doc.16.Req Eu.SAS.77
		Additional operator-specific attributes are allowed.

Subject Public Key Info	[public key], secp256r1	
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 keyAgreement	
Extended Key Usage	**mandatory:** id-kp-safetyCommunication **optional:** serverAuth clientAuth	safetyCommunication OID: 1.3.6.1.45.15.4329 7.3.44.1.100 serverAuth and/or clientAuth depending of the use case of the certificate

Subject Alternative Name	dNSName=[FQDN]
	iPAddress=[IP address]
	URI=[application URI]
		either dNSName or iPAddress shall be used
		if URI is used, it has to uniquely identify the application using the certificate

Field Name	Content	Comment
Certificate Policies	[manufactureroperator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-9 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific distributionPoint]	distributionPoint contains URL to download CRLs within operator networ

[SPPRAMSS-7650]

, SP-SEC-SERVServ-1314.1.2-4 - OHUC

Table 17 Table Operator Human User Certificate (OHUC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA256withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[operator-specific period depending on purpose]	should be configurable based on operational environment. Recommended validity period is 2 years
Subject	**mandatory:** CN=[user identifier] **recommended:** surname=[last name of user] givenName=[first name of user] O=[operator name] C=[operator country]	user identifier is usually an email address. Additional operator-specific attributes are allowed.
Subject Public Key Info	secp256r1, [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)	[key usage depending on use case]	
Extended Key Usage	[extended key usage depending on use case]	

Field Name	Content	Comment
Subject Alternative Name	email=[email address of user]	Note: email is optional to allow complying to privacy legislation. an rfc822Name according to SP-SEC-Serv-2.3-9 - [RFC 5280] chapter 4.2.1.6
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-9 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific distributionPoint]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7651]

, SP-SEC-SERVServ-1314.1.2-5 - OTUC

Table 18 Operator Technical User Certificate (OTUC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA256withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[operator-specific period depending on purpose]	should be configurable based on operational environment. Recommended validity period is 2 years
Subject	**mandatory:** CN=[operator-specific identifier of machine user] **recommended:** O=[operator name] C=[operator country]	Additional operator-specific attributes are allowed
Subject Public Key Info	secp256r1, [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)	[key usage depending on use case]	
Extended Key Usage	[extended key usage depending on use case]	

Field Name	Content	Comment
Subject Alternative Name	[operator-specific]	Optional
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-9 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific distributionPoint]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7652]

, SP-SEC-SERVServ-1314.1.2-6 - OCSC

Table 19 Operator Configuration Signer Certificate (OCSC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA256withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[operator-specific period depending on purpose]	recommended validity period is 2 years

Subject	**mandatory:**
	CN=[unique operator-specific CN]
	recommended:
	OU=[operator-specific organization]
	C=[operator-specific country]
		Additional operator-specific attributes are allowed

Subject Public Key Info	[public key], secp256r1	
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	
Extended Key Usage (critical)	id-kp-configSigning	OID: 1.3.6.1.45.15.43297.443.1.141
Subject Alternative Name	[operator-specific]	optional

Field Name	Content	Comment
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to RFC 5280 SP-SEC-Serv-2.3-9 - [RFC 5280]

[SPPRAMSS-7653]

, SP-SEC-SERVServ-1314.1.2-7 -

Table 20 Operator Trust Anchor Signer Certificate (OTASC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of OSICAC]	
Validity	[manufactureroperator-specific period]	recommended validity period is 1 year

Subject	**mandatory:**
	CN=[unique operator-specific CN]
	recommended:
	OU=[operator-specific organization]
	C=[operator-specific country]
		Additional manufactureroperator-specific attributes are allowed.

Subject Public Key Info	[public key], secp521r1	
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	
Extended Key Usage (critical)	trustanchorSigningid-kp-trustanchorConfigSigning	OID: 1.3.6.1.45.15.43297.443.1.242
Subject Alternative Name	[operator-specific]	optional
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to RFC 5280 SP-SEC-Serv-2.3-9 - [RFC 5280]

[SPPRAMSS-9942]