EU-RAIL SYSTEM PILLAR

Shared Cybersecurity Services Specification

Shared Cybersecurity Services Specification

Author(s)	David Goltzsche , Kooi, Erwin , Richard Poschinger , POYET Nicolas , Wischy, Markus Alexander (SMO RI R&D F IL)
Abstract	Specification of Shared Cybersecurity Interfaces (SCS)
Config Item	System Interface Description
Document ID	Main Documents/SP-SEC-ServSpec#828044 Shared Cybersecurity Services Specification
Classification	Public
Status	In Decision by Steering Group
Version	1.1
Revision	828044
Last Change Date	17.02.2026
Copyright	Brussels: Europe's Rail Joint Undertaking, 2026

Document History

Draft for innovation pillar and SP domain sync 28.06.2023	Wischy, Markus Alexander (SMO RI R&D SYS SEC)	Approved version based on Review X.X
V0.99 Release Candidate 29.01.2025	Goltzsche, David (SMO RI R&D F SEC)	Reviewed version including Change Request
V1.0 05.02.2025	Goltzsche, David (SMO RI R&D F SEC)	Approved version based on Review V0.99 Release Candidate
1.0 25.09.2025	Jorge Block	Approved version based on Review V1.0
1.1 16.02.2026	David Goltzsche	Reviewed version including Findings from Review 1.0.9
1.2 21.01.2026	Goltzsche, David (SMO RI R&D F SEC)	Reviewed version including Findings from Review 1.1

1.1 16.02.2026	David Goltzsche	Reviewed version including Findings from Review 1.0.9
1.2 21.01.2026	Goltzsche, David (SMO RI R&D F SEC)	Reviewed version including Findings from Review 1.1
1.1 16.02.2026	David Goltzsche	Reviewed version including Findings from Review 1.0.9
1.0.9 23.01.2026	Goltzsche, David (SMO RI R&D F SEC)	Reviewed version including Findings from Review 1.1
1.1 16.02.2026	David Goltzsche	Reviewed version including Findings from Review 1.0.9

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

Approval by reviewers

Type of Approval	Document Review

Approval by approvers

Type of Approval	Document Approval

1 Table of Contents

2 Preamble

2.1 Scope, Purpose and Intended Audience

, SP-SEC-Serv-2.1-1 - This specification defines the standard security interfaces (SSI) to the Shared Cybersecurity Services (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
Note2: for an explaination of these abbreviations, see Table 1
Note3: IAM does not cover human user authorization, for this, UAS is used **[**SPPRAMSS-1498 **]**

, SP-SEC-Serv-2.1-2 - A Shared Cybersecurity Service provides common security functions used by other Secure Components. **[**SPPRAMSS-8220 **]**

, SP-SEC-Serv-2.1-3 - The Shared 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-Serv-2.1-4 - 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-Serv-2.1-5 - For a definition of key terms, see Taxonomy and References.
[SPPRAMSS-10317 **]**

2.2 Document Usage

, SP-SEC-Serv-2.2-1 - This specification uses identifiers starting with "SP-SEC-Serv".
[SPPRAMSS-14106 **]**

, SP-SEC-Serv-2.2-2 - Icon types used in this document are defined in SP-SEC-Tax.
[SPPRAMSS-13858 **]**

2.3 References

, 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 **[**SPPRAMSS-13828 **]**

[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 4511]
Lightweight Directory Access Protocol (LDAP): The Protocol

[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

[RFC9113]
HTTP/2

[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 9809]
X.509 Certificate Extended Key Usage (EKU) for Automation

[SP-SEC-CompSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.1

[SP-SEC-CommSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Commmunication Specification, v1.1

[OPC UA-10000-6]
OPC 10000-6: UA Part 6: Mappings

2.4 Terms and Definitions

Secure Component
An implementation, as part of an automation control system, which comprises one or more host devices, embedded devices, network devices or software applications on host devices. A secure component realizes subsystem functions, implements security capabilities, consists of a physical encasing, computing capabilities and network communication, and interfaces 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. **[**SPPRAMSS-1447 **]**

Shared Cybersecurity Services

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>.
[SPPRAMSS-1446 **]**

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).
[SPPRAMSS-6720 **]**

3 Introduction

, SP-SEC-Serv-3-1 - This scheme shows an exemplary hierarchy and interfaces (arrows) of shared services between each other, as well the association to external services. The figure includes:

- the Shared Cybersecurity Services (SCS) which offer mandatory Standard Security Interfaces (SSI) to Secure Components (usage of SSI between the SCS is not mandatory, but recommended)
- 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. Similarly, interfaces between ECS and national services also cross a trust boundary from IT environment to Internet services.

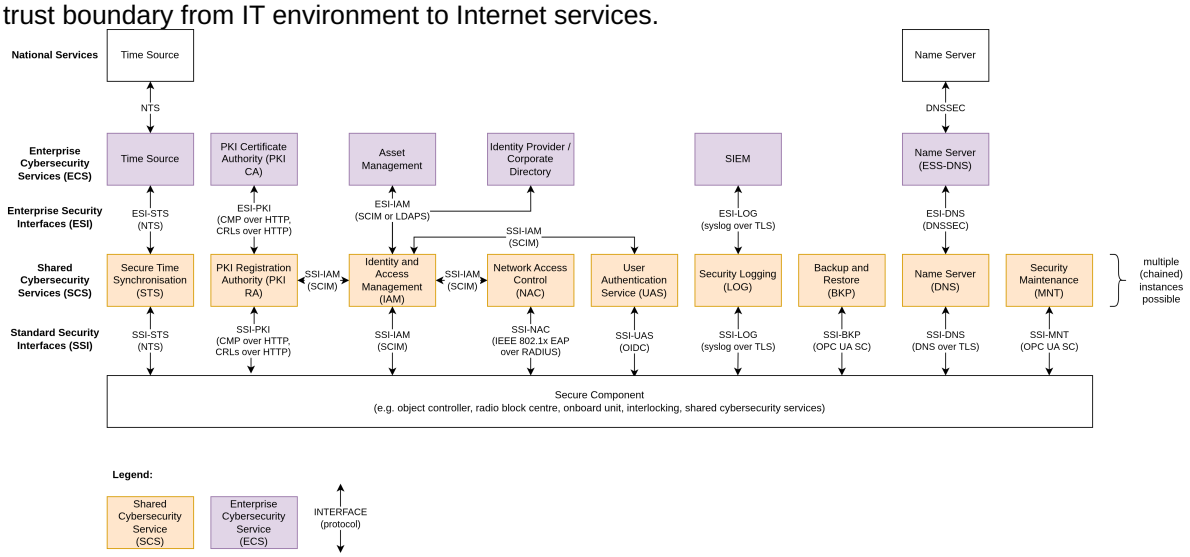

Figure 1 Overview of the Shared Cybersecurity Services and their Interfaces

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. **[**SPPRAMSS-4670 **]**

, SP-SEC-Serv-3-2 - The Shared Cybersecurity Services (SCS) serve as an abstraction layer between the automation environment and the enterprise environment. As the enterprise environment uses IT backoffice technology which is subject to more frequent changes than the automation environment, a key purpose of the SCS is to shield the automation environment from changes in the enterprise environment. It is envisoned to keep the interfaces (SSI) between Secure Components and SCS stable, even when ECS technology and interfaces from ECS to SCS change. This is in line with federated enterprise architectures. **[**SPPRAMSS-16313 **]**

, SP-SEC-Serv-3-3 - 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 = 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	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 certificates)
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)
12 - MNT: Security Maintenance	SSI-MNT	yes	interface for security-related maintenance functions
13 - 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-Serv-3-4 - In the following, the onboard deployment of the Shared Cybersecurity Services is described, which will be refined in a future version of this document.

For the following Shared Cybersecurity Services, an onboard deployment is recommended:

- **STS** - Secure Time Synchronisation

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

A subset of these services requires communication to trackside Shared Cybersecurity Services. This communication might be intermittend. Therefore mechanisms like chaching or federation is recommended.

The following Cybersecurity Services are by default not needed for daily operation and therefore not considered for an onboard deployment:

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

The standardisation of an onboard SSI-MNT interface is currently ongoing, which is therefore not considered.

The train to ground communication is currently being specified (for example in IEC 61375-2-6). The communication for SSI-NTS, SSI-IAM, SSI-LOG, SSI-DNS, SSI-PKI interfaces is expected to be transparently routed between train and infrastructure operated by the railway undertaking owning the train.

The following figure shows an example architecture using these assumptions.

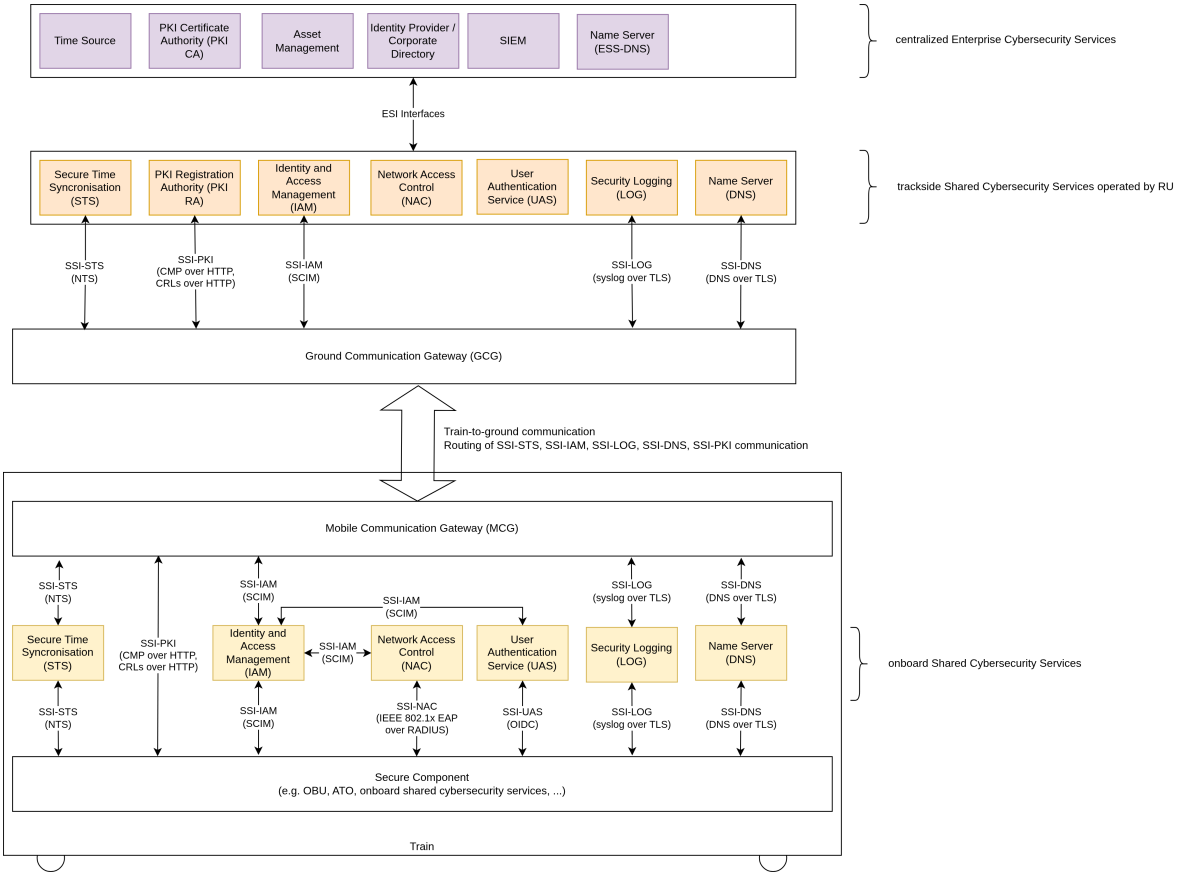

Figure 2 Example architecture of onboard and trackside Shared Cybersecurity Services

For this deployment to work, the availability of roaming in an IP-based mobile network (e.g. FRMCS or 5G) between infrastructure managers (IMs) and railway undertakings (RUs) is assumed, as shown in the following figure.

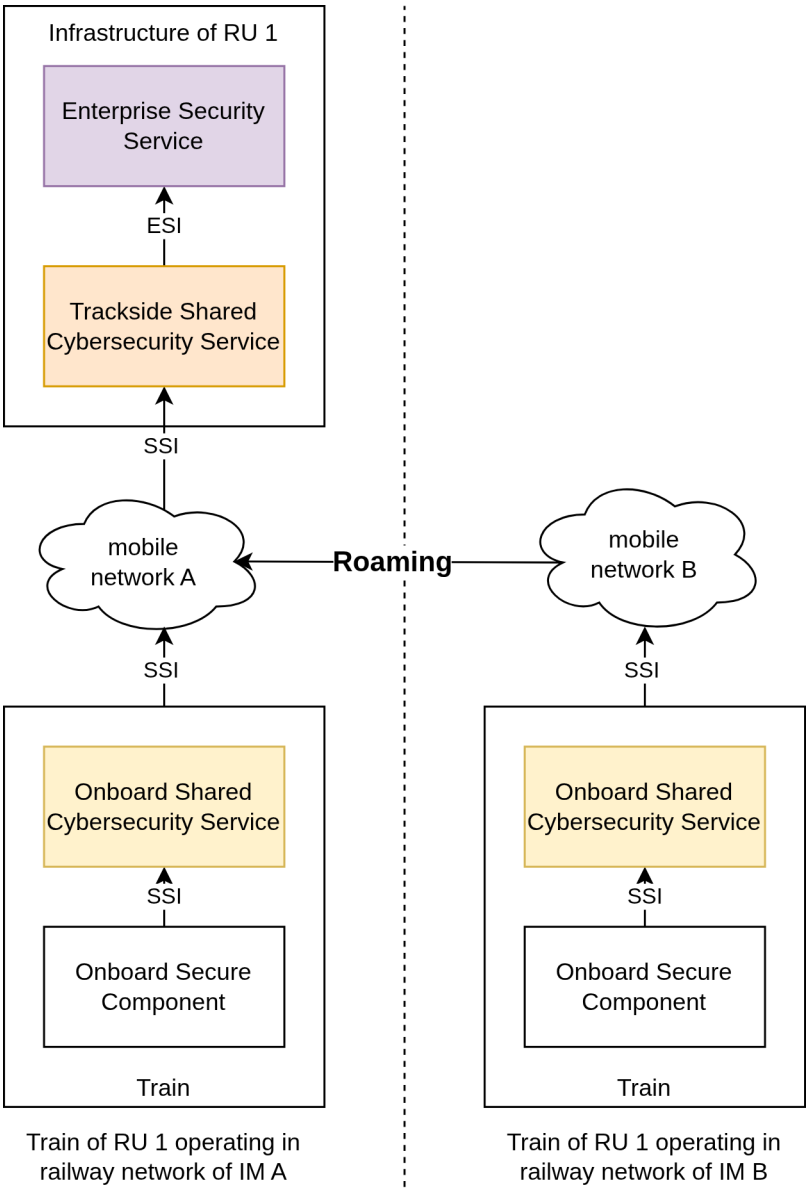

Figure 3 Roaming between networks to reach trackside Shared Cybersecurity Services

[SPPRAMSS-9699 **]**

4 Generic Requirements

, SP-SEC-Serv-4-1 - All implementations of Shared Cybersecurity Services shall fullfill the requirements of the SP-SEC-Serv-2.3-29 - [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 - The SSI interfaces do not require any network 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-2.3-20 - [RFC 8915]
SSI-PKI	CMP over HTTP, CRLs over HTTP	SP-SEC-Serv-2.3-10 - [RFC 5280] SP-SEC-Serv-2.3-26 - [RFC 9483]
SSI-IAM	SCIM 2.0	SP-SEC-Serv-2.3-15 - [RFC 7643] SP-SEC-Serv-2.3-16 - [RFC 7644]
SSI-NAC	IEEE 802.1x EAP over RADIUS	SP-SEC-Serv-2.3-5 - [IEEE 802.1X-2020] SP-SEC-Serv-2.3-23 - [RFC 9190] SP-SEC-Serv-2.3-7 - [RFC 2865]
SSI-LOG	syslog over TLS	SP-SEC-Serv-2.3-12 - [RFC 5425] SP-SEC-Serv-2.3-27 - [RFC 9662]
SSI-UAS	OIDC	SP-SEC-Serv-2.3-4 - [OIDC 1.0]
SSI-BKP	OPC UA	SP-SEC-Serv-2.3-31 - [OPC UA-10000-6] SP-SEC-Serv-2.3-21 - [RFC9113]
SSI-MNT	OPC UA	SP-SEC-Serv-2.3-31 - [OPC UA-10000-6]
SSI-DNS	DNS over TLS	SP-SEC-Serv-2.3-17 - [RFC 7858]

[SPPRAMSS-11178 **]**

, 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-2.3-20 - [RFC 8915]
ESI-PKI	CMP over HTTP, CRLs over HTTP	SP-SEC-Serv-2.3-10 - [RFC 5280] SP-SEC-Serv-2.3-26 - [RFC 9483]
ESI-IAM	SCIM 2.0 via HTTPS or LDAPS with TLS	SP-SEC-Serv-2.3-16 - [RFC 7644] SP-SEC-Serv-2.3-9 - [RFC 4511]
ESI-LOG	syslog over TLS	SP-SEC-Serv-2.3-12 - [RFC 5425] SP-SEC-Serv-2.3-27 - [RFC 9662]
ESI-DNS	DNSSEC	SP-SEC-Serv-2.3-24 - [RFC 9364]

[SPPRAMSS-11983 **]**

, SP-SEC-Serv-4-5 - Seperate deployment of the SCS and ECS by network segmentation (e.g. a DMZ) is recommended. **[**SPPRAMSS-16014 **]**

5 STS: Secure Time Synchronisation

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

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

[SPPRAMSS-3828 **]**

5.1 NTS Architectural Overview

📄**, SP-SEC-Serv-5.1-1 -**

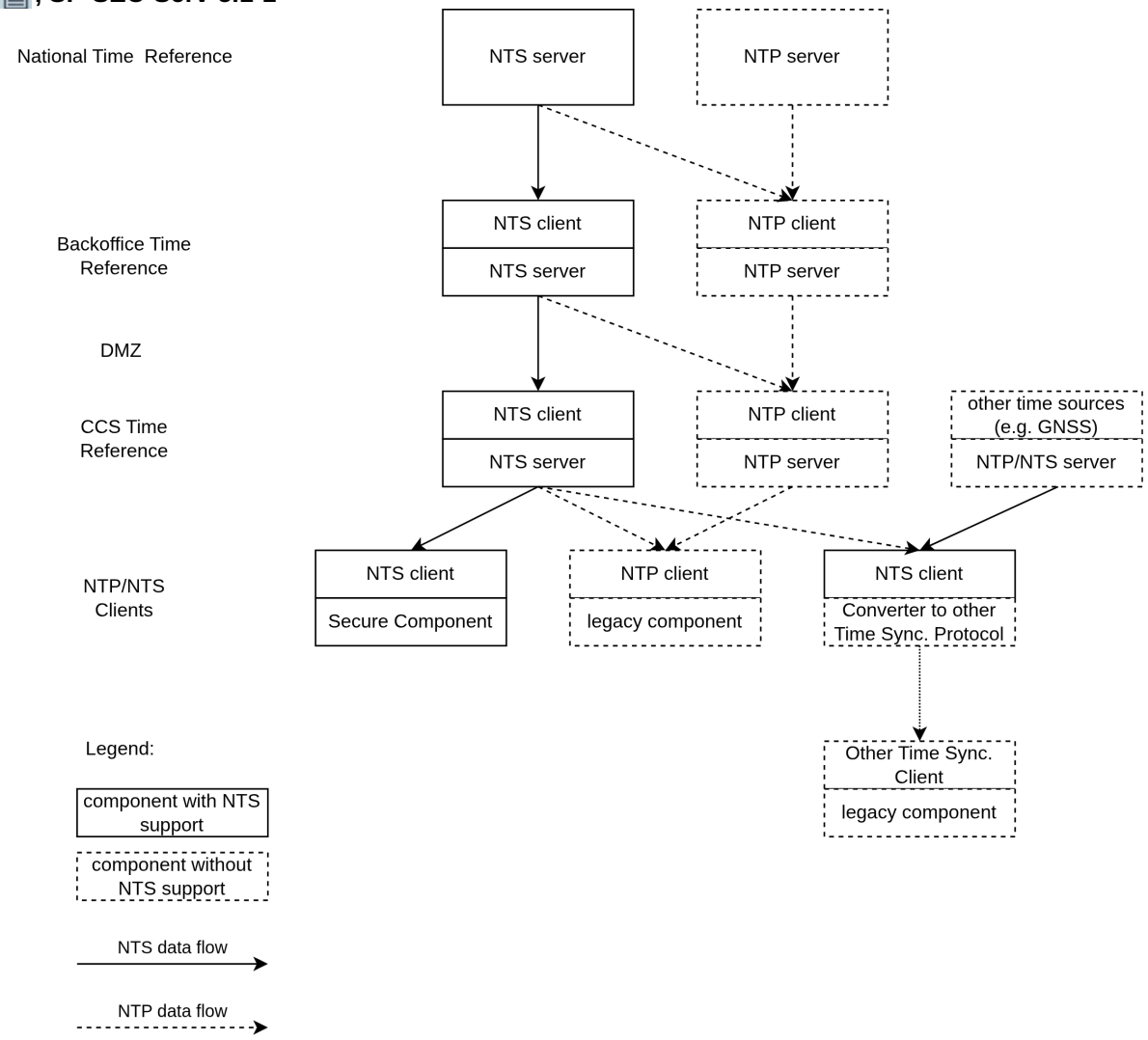

Figure 4 Exemplary hierarchy of NTS servers

[SPPRAMSS-3702 **]**

5.2 Server Requirements

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

, SP-SEC-Serv-5.2-2 - The SCS-STS shall use Network Time Security (NTS) as specified in SP-SEC-Serv-2.3-20 - [RFC 8915].
Note: This means, that at least TLS version 1.3 is used. **[**SPPRAMSS-9965 **]**

, SP-SEC-Serv-5.2-3 - The SCS-STS shall use the fixed network ports defined in SP-SEC-Serv-2.3-20 - [RFC 8915].
Note: This means that NTPv4 Port Negotiation is not used. **[**SPPRAMSS-3716 **]**

, SP-SEC-Serv-5.2-4 - The SCS-STS shall use a Operator Non-Safety Communication Certificate (ONCC) as server certificate as defined in 6.2.2 - Operator Certificates. **[**SPPRAMSS-5264 **]**

, SP-SEC-Serv-5.2-5 - The SCS-STS shall only accept NTS-KE requests from authenticated clients. **[**SPPRAMSS-5266 **]**

5.3 Client Requirements

, SP-SEC-Serv-5.3-1 - The SSI-STS client shall use NTS as specified in SP-SEC-Serv-2.3-20 - [RFC 8915] .
Note: This means, that at least TLS version 1.3 is used. **[**SPPRAMSS-3701 **]**

, SP-SEC-Serv-5.3-2 - The SSI-STS client shall use a Operator Non-Safety Communication Certificate (ONCC) as defined in 6.2.2 - Operator Certificates for client authentication. **[**SPPRAMSS-5265 **]**

, SP-SEC-Serv-5.3-3 - During commissioning, the SSI-STS client shall use NTP as specified in SP-SEC-Serv-2.3-13 - [RFC 5905] .
Note: this removes the circular dependency when requesting the first operator certificates. **[**SPPRAMSS-13367 **]**

5.4 Backwards Compatibility to NTP

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).

6 PKI: Public Key Infrastructure

, SP-SEC-Serv-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. **[**SPPRAMSS-3690 **]**

, SP-SEC-Serv-6-2 - The following Figure shows interfaces and protocols used between the PKI and Secure Components. The Secure Components clients establish a TLS connection using the certificates distributed by the PKI.

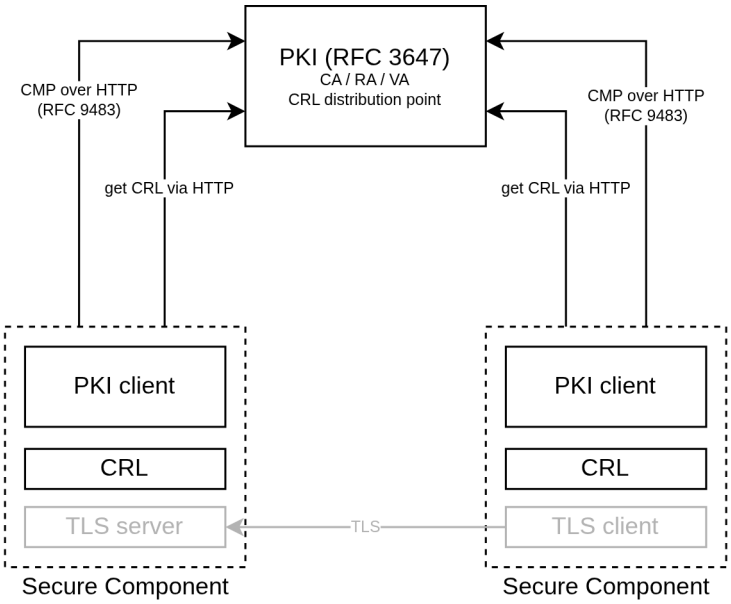

Figure 5 Interface between PKI and Secure Components

[SPPRAMSS-3393 **]**

6.1 Use Cases

6.1.1 Use Case: Commissioning

, SP-SEC-Serv-6.1.1-1 - SP-Sec-Comp-5.5.4 describes the commissioning process of new component to an installation. The Secure Component authenticates itself to the Registration Authority (RA) with a Manufacturer Device Certificate (MDC, see 6.2.1 - Manufacturer Certificates) to request the Operator Device Certificate (ODC, see 6.2.2 - Operator Certificates) according to Sections 4.1.1 and 5.2.1 of SP-SEC-Serv-2.3-26 - [RFC 9483]. With the ODC, further operator certificates can be obtained according to Sections 4.1.2 and 5.2. of SP-SEC-Serv-2.3-26 - [RFC 9483]. **[**SPPRAMSS-5086 **]**

6.1.2 Use Case: Obtaining additional Operator Certificates

, SP-SEC-Serv-6.1.2-1 - The following Figure shows the dependencies of certificates. The Certificate Management Protocol (CMP as defined in SP-SEC-Serv-2.3-26 - [RFC 9483]) is used to request further certificates. Thereby, the previous certificate is used to authenticate the device before requesting following certificates. This is to ensure (a) device identity binding using the Manufacturer Device Certificate (MDC), (b) proof-of-possession of the key, (c) integrity and freshness of all enrollment messages. Since the Manufacturer Device Certificate (MDC) is installed during manufacturing, the device always has the

possibility to request the other certificates.

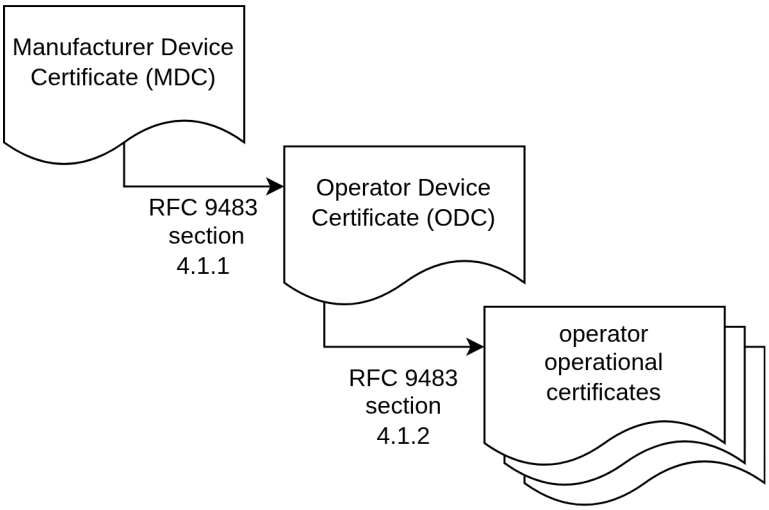

Figure 6 Depedencies of Certificates with References to CMP RFC

[SPPRAMSS-5845 **]**

6.1.3 Use Case: Updating Operator Certificates

, SP-SEC-Serv-6.1.3-1 - Operator Certificates can be updated before their validity ends according to SP-SEC-Serv-2.3-26 - [RFC 9483] section 4.1.3. **[**SPPRAMSS-10182 **]**

6.1.4 Use Case: Revoking Operator Certificates

, SP-SEC-Serv-6.1.4-1 - Operator Certificates can be revoked according to SP-SEC-Serv-2.3-26 - [RFC 9483] section 5.3.2. **[**SPPRAMSS-10183 **]**

6.2 Certificates

, SP-SEC-Serv-6.2-1 - All certificates in the PKI hierarchy shall be based on Elliptic Curve Cryptography (ECC).
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). **[**SPPRAMSS-10177 **]**

, SP-SEC-Serv-6.2-2 - The certificate profiles (see 14.1 - Certificate Profiles) use the following Object Identifiers (OIDs) defined in SP-SEC-Serv-2.3-28 - [RFC 9809] in the Extended Key Usage (EKU) field.

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

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

6.2.1 Manufacturer Certificates

, SP-SEC-Serv-6.2.1-1 - 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.

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

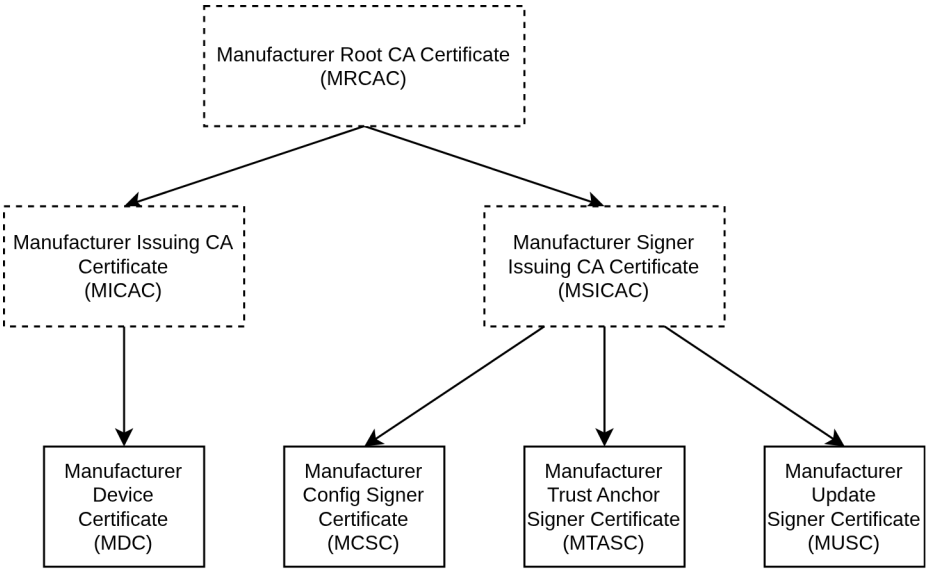

Figure 7 Manufacturer PKI Hierarchy. Certificates with solid lines are defined by certificate profiles.
[SPPRAMSS-5650 **]**

, SP-SEC-Serv-6.2.1-2 - The following table lists the 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 Occurrence
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
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-6.2.1-3 - The Manufacturer Device Certificate (MDC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.1-1. **[**SPPRAMSS-7645 **]**

, SP-SEC-Serv-6.2.1-4 - The Manufacturer Config Signer Certificate (MCSC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.1-2. **[**SPPRAMSS-7356 **]**

, SP-SEC-Serv-6.2.1-5 - The Manufacturer Trust Anchor Signer Certificate (MTASC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.1-3.
[SPPRAMSS-7404 **]**

, SP-SEC-Serv-6.2.1-6 - The Manufacturer Update Signer Certificate (MUSC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.1-4. **[**SPPRAMSS-7405 **]**

, SP-SEC-Serv-6.2.1-7 - The Manufacturer CA certificates shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.3-1 - Table # CA Certificate profile.
Note: this only applies to root, intermediate and issuing CA certificates, not to leaf certificates **[**SPPRAMSS-16109 **]**

, SP-SEC-Serv-6.2.1-8 - Signatures created with the Manufacturer Configuration Signer Certificate (MCSC), Manufacturer Trust Anchor Signer Certificate (MTASC), Manufacturer Update Signer Certificate (MUSC) shall use the signature algorithm ecdsa-with-SHA512. **[**SPPRAMSS-16314 **]**

6.2.2 Operator Certificates

, SP-SEC-Serv-6.2.2-1 - 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, OUC, OCSC, OTASC), the exact numbers and characteristics of root and issuing CAs can be defined by the operator.
Note: trust anchors are usually associated with a root CA, but this is not a requirement

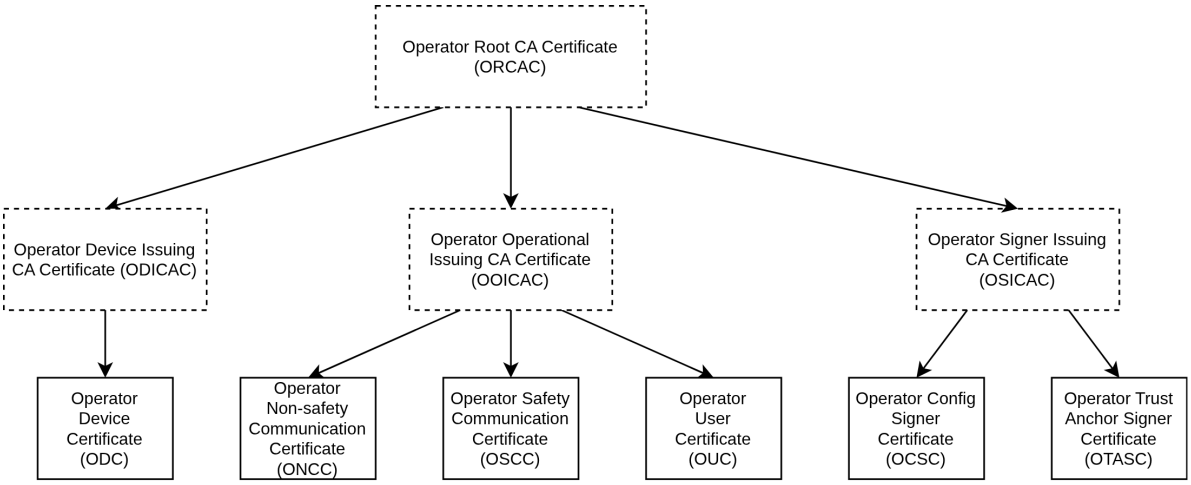

Figure 8 Operator PKI Hierarchy (ECC). Certificates with solid lines are defined by certificate profiles.

[SPPRAMSS-5126 **]**

, SP-SEC-Serv-6.2.2-2 - 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 Occurrence
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.	one or multiple ONCCs per software process realising non-safety communication
Operator Safety Communication Certificate	OSCC	OSCCs are used to protect safety communication.	one or multiple OSCCs per software process realising safety communication
Operator User Certificate	OUC	OUCs are used by human users or software processes, e.g. for authentication and authorisation.	zero to multiple OUCs per human user/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-6.2.2-3 - The Operator Device Certificate (ODC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.2-1. **[**SPPRAMSS-8001 **]**

, SP-SEC-Serv-6.2.2-4 - The Operator Non-Safety Communication Certificate (ONCC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.2-2. **[**SPPRAMSS-5129 **]**

, SP-SEC-Serv-6.2.2-5 - The Operator Safety Communication Certificate (OSCC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.2-3. **[**SPPRAMSS-5131 **]**

, SP-SEC-Serv-6.2.2-6 - The Operator User Certificate (OUC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.2-4. **[**SPPRAMSS-5123 **]**

, SP-SEC-Serv-6.2.2-7 - The OUC shall be protected with a second factor.
Note: This second factor can be a passphrase or PIN. **[**SPPRAMSS-16015 **]**

, SP-SEC-Serv-6.2.2-8 - The Operator Configuration Signer Certificate (OCSC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.2-5. **[**SPPRAMSS-5270 **]**

, SP-SEC-Serv-6.2.2-9 - The Operator Trust Anchor Signer Certificate (OTASC) shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.2-6 **[**SPPRAMSS-9943 **]**

, SP-SEC-Serv-6.2.2-10 - The Operator CA certificates shall fulfill the certificate profile defined in SP-SEC-Serv-14.1.3-1 - Table # CA Certificate profile.
Note: this only applies to root, intermediate and issuing CA certificates, not to leaf certificates **[**SPPRAMSS-16110 **]**

, SP-SEC-Serv-6.2.2-11 - Signatures created with the Operator Configuration Signer Certificate (OCSC), and Operator Trust Anchor Signer Certificate (OTASC) shall use the signature algorithm ecdsa-with-SHA512. **[**SPPRAMSS-16348 **]**

6.3 PKI CA/RA requirements

, SP-SEC-Serv-6.3-1 - The PKI CA mentioned in this chapter is the CA installed in the operators environment, not the manufacturer CA. **[**SPPRAMSS-11962 **]**

, SP-SEC-Serv-6.3-2 - The SSI-PKI shall issue X.509 v3 certificates as defined in SP-SEC-Serv-2.3-10 - [RFC 5280]. **[**SPPRAMSS-6744 **]**

, SP-SEC-Serv-6.3-3 - The SSI-PKI shall issue certificates according to the certificate profiles defined in 14.1 - Certificate Profiles. **[**SPPRAMSS-6745 **]**

, SP-SEC-Serv-6.3-4 - The PKI RA/CA shall provide the capability to issue and rekey certificates using the CMP protocol version 2 via HTTP according to the Lightweight CMP Profile (LCMPP) as defined in SP-SEC-Serv-2.3-26 - [RFC 9483].
[SPPRAMSS-4062 **]**

, SP-SEC-Serv-6.3-5 - The PKI RA/CA shall support the following CMP messages: Initialization Request (ir), Certification Request (cr), Key Update Request (kur), Certificate Confirmation (certConf) and their associated responses (ip, cp, kup, pkiConf, error).
Note: These CMP messages represent a subset of the messages defined in SP-SEC-Serv-2.3-26 - [RFC 9483].
[SPPRAMSS-4064 **]**

, SP-SEC-Serv-6.3-6 - The PKI RA/CA shall validate the content and signature-based message protection of every received CMP request according to Section 3.5 in SP-SEC-Serv-2.3-26 - [RFC 9483] before accepting it. **[**SPPRAMSS-6604 **]**

, SP-SEC-Serv-6.3-7 - The PKI RA/CA shall send a pkiConf message at the reception of the certConf message.
Note: this means that implicitConfirm is not used. **[**SPPRAMSS-4142 **]**

, SP-SEC-Serv-6.3-8 - The PKI RA/CA shall provide the following CMP endpoints according to Section 6.1 of SP-SEC-Serv-2.3-26 - [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
`/.well-known/cmp/p/OSCC/certification`	OSCC	CMP message protection with ODC CMP responses: message protection with issuing CA key

[SPPRAMSS-5167 **]**

, SP-SEC-Serv-6.3-9 - The PKI RA/CA shall provide the following CMP endpoints with the listed endpoint protection according to Section 6.1 of SP-SEC-Serv-2.3-26 - [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-Serv-6.3-10 - The PKI RA shall only process authenticated and authorized CMP requests. **[**SPPRAMSS-5223 **]**

, SP-SEC-Serv-6.3-11 - The PKI RA/CA shall support the following protection algorithms for creating signatures to protect its CMP responses: ecdsa-with-SHA256, ecdsa-with-SHA512 according to Section 3.2 of SP-SEC-Serv-2.3-25 - [RFC 9481].
Note: SP-SEC-Serv-6.3-8 and SP-SEC-Serv-6.3-9 define which key to use for every CMP endpoint. **[**SPPRAMSS-7494 **]**

, SP-SEC-Serv-6.3-12 - The PKI RA/CA shall reject CMP protection algorithms not defined in this specification. **[**SPPRAMSS-15419 **]**

, SP-SEC-Serv-6.3-13 - The PKI RA shall only forward CMP initialization requests to PKI CA if signed by an MDC which associated asset exists in the SCS-IAM and the asset's state is "COMMISSIONING". **[**SPPRAMSS-15437 **]**

, SP-SEC-Serv-6.3-14 - The PKI RA shall only forward CMP certification requests to PKI CA if signed by an ODC which associated asset exists in the SCS-IAM and the asset's state is "ACTIVE". **[**SPPRAMSS-15435 **]**

, SP-SEC-Serv-6.3-15 - If the PKI RA is not forwarding a initialization request due to an SCS-IAM status mismatch, the PKI RA shall respond with an initialization response containing the PKIStatus "rejection". **[**SPPRAMSS-15436 **]**

, SP-SEC-Serv-6.3-16 - If the PKI RA is not forwarding a certification request due to an SCS-IAM status mismatch, the PKI RA shall respond with a certification response containing the PKIStatus "rejection". **[**SPPRAMSS-15434 **]**

, SP-SEC-Serv-6.3-17 - The PKI RA/CA shall provide CRLs compliant to SP-SEC-Serv-2.3-10 - [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-6.3-18 - CRLs provided by the PKI RA/CA shall contain the nextUpdate field.
Note: recommended update period is 24h. **[**SPPRAMSS-7629 **]**

6.4 PKI Client Requirements

, SP-SEC-Serv-6.4-1 - The SSI-PKI client shall provide the capability to request and rekey certificates using the CMP protocol version 2 via HTTP according to the Lightweight CMP Profile (LCMPP) SP-SEC-Serv-2.3-26 - [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. **[**SPPRAMSS-4070 **]**

, SP-SEC-Serv-6.4-2 - 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-2.3-26 - [RFC 9483] Section 4.1.3). **[**SPPRAMSS-7177 **]**

, SP-SEC-Serv-6.4-3 - The SSI-PKI client shall sign CMP requests by using ecdsa-with-sha256 as protectionAlg as defined in Section 3.2 of SP-SEC-Serv-2.3-25 - [RFC 9481] .
[SPPRAMSS-7496 **]**

, SP-SEC-Serv-6.4-4 - The SSI-PKI client shall support the following CMP messages: Initialization request (ir), Certification Request (cr), Key Update Request (kur), Certificate Confirmation (certConf) and their associated responses (ip, cp, kup, pkiConf, error) as defined in SP-SEC-Serv-2.3-26 - [RFC 9483] .
[SPPRAMSS-4068 **]**

, SP-SEC-Serv-6.4-5 - The SSI-PKI client shall validate the content and signature-based message protection of every received CMP message according to SP-SEC-Serv-2.3-26 - [RFC 9483] section 3.5 before accepting it.
Note: Any error condition should be handled according to SP-SEC-Serv-2.3-26 - [RFC 9483] Section 3.6.1. **[**SPPRAMSS-9670 **]**

, SP-SEC-Serv-6.4-6 - The SSI-PKI client shall request and rekey certificates needed for operation. **[**SPPRAMSS-4069 **]**

, SP-SEC-Serv-6.4-7 - The SSI-PKI client shall download CRLs via HTTP and process CRLs as defined in SP-SEC-Serv-2.3-10 - [RFC 5280] using a URL defined in the CRL Distribution Point (CDP) extension, which can be overwritten by a URL defined in the client's configuration. **[**SPPRAMSS-4067 **]**

, SP-SEC-Serv-6.4-8 - The PKI client shall support the following protection algorithms for creating signatures to protect its CMP requests: ecdsa-with-SHA256, ecdsa-with-SHA512 according to Section 3.2 of SP-SEC-Serv-2.3-25 - [RFC 9481].
Note: SP-SEC-Serv-6.3-8 and SP-SEC-Serv-6.3-9 define which key to use for every CMP endpoint.
[SPPRAMSS-7495 **]**

7 IAM: Identity and Access Management

The SSI-IAM is an interface for managing digital identities (human users, software processes or devices). This eliminates the need for credential stores on individual components. The IAM acts as a single source of truth for identification and 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-Serv-7-2 - The SCS-IAM shall be able to synchronise its asset database via ESI-IAM with an asset management system. **[**SPPRAMSS-11439 **]**

, SP-SEC-Serv-7-3 - The SCS-IAM shall be able to synchronise its user database via ESI-IAM with a corporate directory. **[**SPPRAMSS-7974 **]**

, SP-SEC-Serv-7-4 - The SCS-IAM 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-Serv-7-5 - The SCS-IAM shall have the capability to retrieve authorisation information from an authorisation store (e.g. a training database for maintainers). **[**SPPRAMSS-4976 **]**

, SP-SEC-Serv-7-6 - The OPC UA permissions for SSI are defined in Chapter 4 of the SP-SEC-Serv-2.3-30 - [SP-SEC-CommSpec]. **[**SPPRAMSS-9806 **]**

, SP-SEC-Serv-7-7 - 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-Serv-7-8 - The SCS-IAM shall accept SCIM 2.0 requests over REST over HTTPS according to SP-SEC-Serv-2.3-16 - [RFC 7644].
[SPPRAMSS-5803 **]**

, SP-SEC-Serv-7-9 - The SCS-IAM shall use an Operator Non-safety Communication Certificate (ONCC). **[**SPPRAMSS-5811 **]**

, SP-SEC-Serv-7-10 - The SSI-IAM client shall use an Operator Non-safety Communication Certificate (ONCC). **[**SPPRAMSS-15506 **]**

, SP-SEC-Serv-7-11 - The SCS-IAM shall send SCIM 2.0 JSON-formatted responses as defined in SP-SEC-Serv-2.3-16 - [RFC 7644]. **[**SPPRAMSS-5802 **]**

, SP-SEC-Serv-7-12 - The SCS-IAM shall send SCIM 2.0 responses following the Core Schema defined in SP-SEC-Serv-2.3-15 - [RFC 7643] . **[**SPPRAMSS-10351 **]**

7.1 Asset Inventory

, SP-SEC-Serv-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-7.1-12)

[SPPRAMSS-11371 **]**

, SP-SEC-Serv-7.1-3 - The SSI-IAM server shall distinguish the following Secure Component types by assigning the following permissions:

Secure Component Type	Permissions
PKI RA	`eu.rail.security.iam.asset-info` `eu.rail.security.iam.update-assets-certificates`
All authenticated components	`eu.rail.security.iam.asset-info`

Note: mapping these permissions to roles, which match to component types is allowed
[SPPRAMSS-9807 **]**

, SP-SEC-Serv-7.1-4 - The servers implementing SSI-PKI RA, SSI-NAC or Update Server (according to SMI) shall support the ability to request data of an asset by sending an HTTP GET request to the SSI-IAM interface with a filter that includes either serial number from the MDC (as `serialNumber` attribute) 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: an MDC-based request has the following form:

```
GET /v2/Assets?filter=(serialNumber eq "[serial number]") and (manufacturerDN eq "[manufacturer-specific DN]") HTTP/1.1
Host: [SSI-IAM instance address]
User-Agent: [SSI-IAM REST Client identifier]
Accept: application/scim+json
```

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

```
GET /v2/Assets?filter=(CN eq "[CN]") HTTP/1.1
Host: [SSI-IAM instance address]
User-Agent: [SSI-IAM REST Client identifier]
Accept: application/scim+json
```

[SPPRAMSS-5805 **]**

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

, SP-SEC-Serv-7.1-6 - If the SCS-IAM 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. **[**SPPRAMSS-13066 **]**

, SP-SEC-Serv-7.1-7 - The SCS-IAM shall implement the schema `urn:ietf:params:scim:eu-rail:2.0:Asset` defined by the following JSON object:

```
{
"id": "urn:ietf:params:scim:eu-rail:2.0:Asset",
"name": "Asset",
"description": "Asset Schema",
"attributes": [
{
"name": "serialNumber",
"type": "string",
"multiValued": false,
"required": true,
"caseExact": true,
"mutability": "immutable",
"returned": "default",
"uniqueness": "none",
"description": "serial number of the asset provided in the MDC"
},
{
"name": "CN",
"type": "string",
"multiValued": false,
"required": false,
"caseExact": true,
"mutability": "readWrite",
"returned": "default",
"uniqueness": "server",
"description": "Common Name of the asset as part of the ODC"
},
{
"name": "manufacturerDN",
"type": "string",
"multiValued": false,
"required": true,
"caseExact": true,
"mutability": "immutable",
"returned": "default",
"uniqueness": "none",
"description": "Distinguished Name of the root CA certificate corresponding to the MDC"
},
{
"name": "status",
"type": "string",
```

```
"multiValued": false,
"required": true,
"caseExact": true,
"mutability": "readWrite",
"returned": "always",
"uniqueness": "none",
"canonicalValues": ["CREATED","ACTIVE","INACTIVE","COMMISSIONING","DECOMMISSIONED"],
"description": "state of the asset"
},
{
"name" : "entitlements",
"type" : "complex",
"multiValued" : true,
"description" : "A list of entitlements for the User that represent a thing the User has.",
"required" : false,
"subAttributes" : [
{
"name" : "value",
"type" : "string",
"multiValued" : false,
"description" : "The value of an entitlement.",
"required" : true,
"caseExact" : false,
"mutability" : "readWrite",
"returned" : "default",
"uniqueness" : "none"
},
"mutability" : "readWrite",
"returned" : "default"
},
{
"name": "certificates",
"type": "complex",
"subattributes": [
{
"name": "type",
"type": "string",
"multiValued": false,
"required": true,
"caseExact": true,
"mutability": "immutable",
"returned": "default",
"uniqueness": "none",
"canonicalValues": ["ODC","ONCC","OSCC","OUC","OCSC","OTASC"],
"description": "Certificate Profile Tag"
},
```

```
{
"name": "serialNumber",
"type": "integer",
"multiValued": false,
"required": true,
"caseExact": true,
"mutability": "immutable",
"returned": "default",
"uniqueness": "none",
"description": "serial number of the certificate according to RFC 5280 4.1.2.2"
},
{
"name": "CN",
"type": "string",
"multiValued": false,
"required": true,
"caseExact": true,
"mutability": "immutable",
"returned": "default",
"uniqueness": "none",
"description": "common name of the certificate"
},
{
"name": "value",
"type": "string",
"multiValued": false,
"required": true,
"caseExact": false,
"mutability": "immutable",
"returned": "default",
"uniqueness": "none",
"description": "base64-encoded DER string of the X.509 certificate (without BEGIN CERTIFICATE/END
CERTIFICATE)"
}
],
"multiValued": true,
"required": true,
"caseExact": true,
"mutability": "readWrite",
"returned": "default",
"uniqueness": "none",
"description": "Certificates issued for the asset"
}
]
}
```


Note: additional attributes are allowed **[**SPPRAMSS-15429 **]**

, SP-SEC-Serv-7.1-8 - If the SCS-IAM has a record of the requested asset, 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:eu-rail:2.0:Asset` (see SP-SEC-Serv-7.1-7), which includes the `serialNumber` or `CN` attribute as asset identifier.

Note1: a response with `serialNumber` attribute 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:eu-rail:2.0:Asset"],
		"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\""
		},
		"serialNumber":"<asset identifier>",
		"manufacturerDN":"<DN of manufacturer>",
		"status":"<asset status>",
		"entitlements": "<asset entitlements>",
		"certificates": " "<asset certificates>"
	],

}
]
}
```

Note2: a response with `CN` attribute 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:eu-rail:2.0:Asset"],
		"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>",
		"status":"<asset status>",
		"entitlements": "<asset entitlements>",
		"certificates": " "<asset certificates>"
```

```
      ],

}
]
}
```

Note3: additional attributes are allowed **[**SPPRAMSS-9842 **]**

, SP-SEC-Serv-7.1-9 - The SCS-IAM shall support the following states for assets: CREATED**,** ACTIVE, INACTIVE, COMMISSIONING, DECOMMISSIONED. **[**SPPRAMSS-15431 **]**

, SP-SEC-Serv-7.1-10 - The SCS-IAM shall support the state changes for assets as depicted in the following figure:

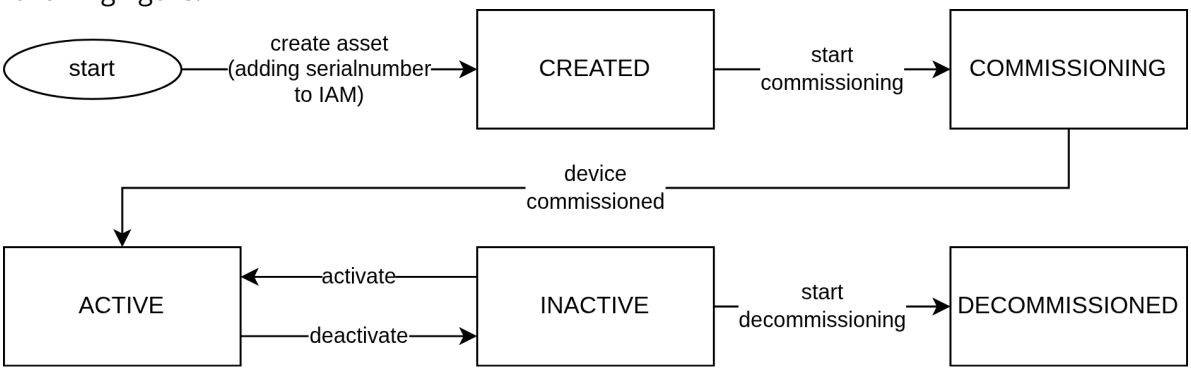

Figure 9 asset state transitions for SCS-IAM

[SPPRAMSS-15430 **]**

, SP-SEC-Serv-7.1-11 - If the SCS-IAM has no record of the requested asset, the SCS-IAM shall return a SCIM response with the schema `urn:ietf:params:scim:api:messages:2.0:ListResponse`, containing totalResults set to 0 and an empty Resources list.

Note: 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":0,
      "Resources": [
]
}
```

[SPPRAMSS-6709 **]**

, SP-SEC-Serv-7.1-12 - The 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 SCIM request 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 **[**SPPRAMSS-6710 **]**

, SP-SEC-Serv-7.1-13 - If the SSI-IAM successfully added the supplied certificate to the assets resource, the SSI-IAM shall return a SCIM response with the schema `urn:ietf:params:scim:api:messages:2.0:ListResponse` as defined in SP-SEC-Serv-7.1-8 **[**SPPRAMSS-6715 **]**

, SP-SEC-Serv-7.1-14 - If the SCS-IAM successfully added a supplied ODC with status "issued" and if the corresponding asset is in status "COMMISSIONING", the SCS-IAM shall set the status of the corresponding asset to "ACTIVE". **[**SPPRAMSS-15511 **]**

7.2 User Inventory

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

, SP-SEC-Serv-7.2-2 - The SSI-IAM 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)

[SPPRAMSS-11372 **]**

, 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
[SPPRAMSS-11373 **]**

, SP-SEC-Serv-7.2-4 - The SSI-IAM client shall support the ability to retrieve user permissions from the SSI-IAM by sending an HTTP GET request to the SSI-IAM interface with a filter that includes the email 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,entitlements cn HTTP/
1.1
Host: [SSI-IAM instance address]
User-Agent: [SSI-IAM REST Client identifier]
Accept: application/scim+json
```

[SPPRAMSS-9817 **]**

, SP-SEC-Serv-7.2-5 - If the SSI-IAM can provide the requested user 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.rail.sdi.diagnostic-read"},
            {"value": "eu.rail.ssi.security-read"}
            ]
      ],
}
]
}
```

Note2: additional attributes are allowed **[**SPPRAMSS-9818 **]**

8 NAC: Network Access Control

, SP-SEC-Serv-8-1 - The purpose of the SSI Network Access Control (SSI-NAC) interface is to prevent unauthorized access to the network. The SCS-NAC 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.

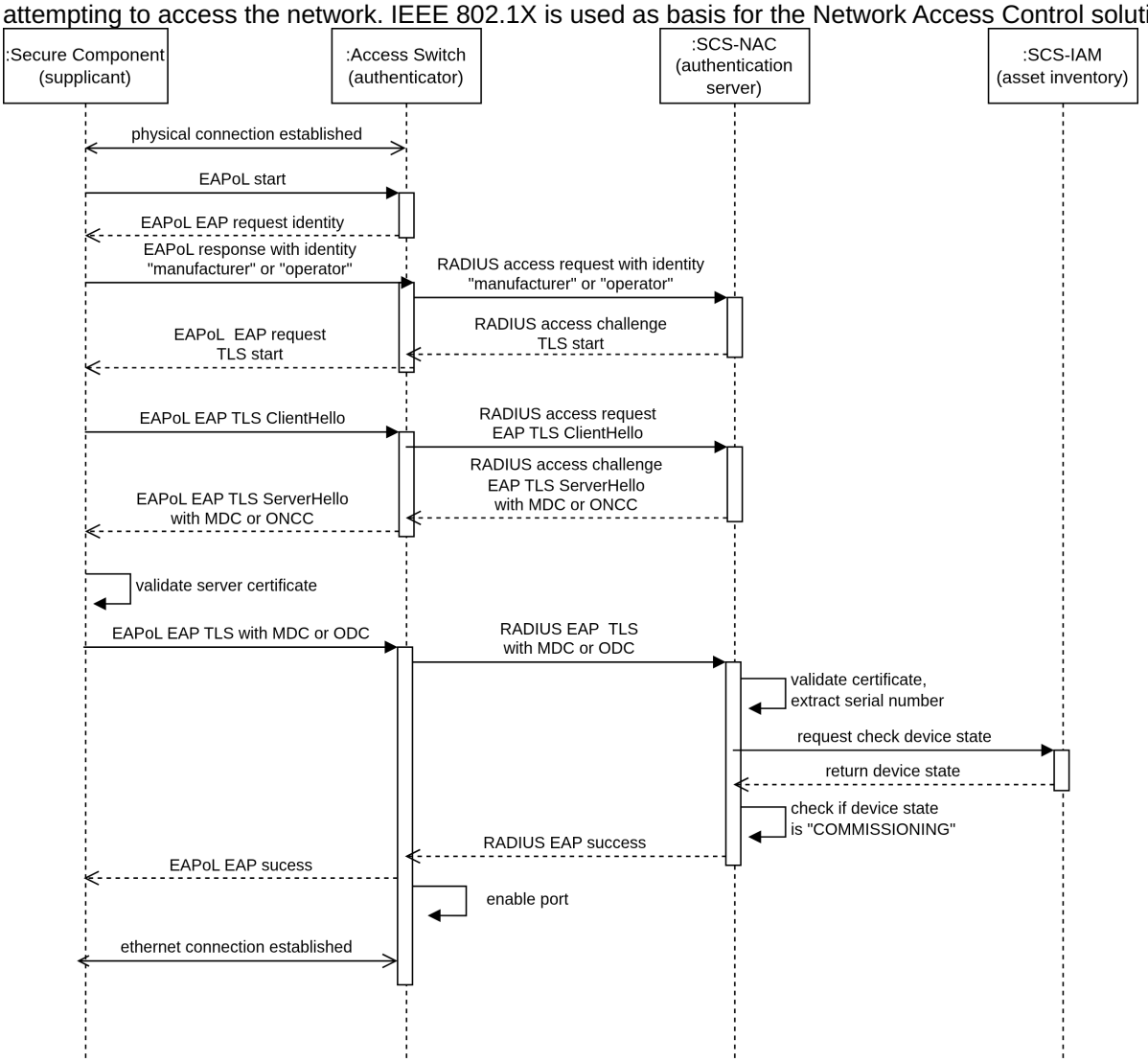

Figure 10 Network authentication sequence diagram **[**SPPRAMSS-4814 **]**

, SP-SEC-Serv-8-2 - The SSI-NAC interface shall realize network authentication using SP-SEC-Serv-2.3-5 - [IEEE 802.1X-2020]. **[**SPPRAMSS-10039 **]**

, SP-SEC-Serv-8-3 - The SSI-NAC interface shall realize the EAP-TLS protocol as described in SP-SEC-Serv-2.3-23 - [RFC 9190]. **[**SPPRAMSS-4817 **]**

, SP-SEC-Serv-8-4 - 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-8-5 - The SCS-NAC shall reply to RADIUS requests using the ODC to authenticate itself towards the Secure Component. **[**SPPRAMSS-4897 **]**

, SP-SEC-Serv-8-6 - The SCS-NAC shall extract the serial number of the MDC of the requesting Secure Component (see SP-SEC-Serv-14.1.1-1). **[**SPPRAMSS-4945 **]**

, SP-SEC-Serv-8-7 - The SCS-NAC shall extract the CN of the ODC of the requesting Secure Component (see SP-SEC-Serv-14.1.2-1). **[**SPPRAMSS-13065 **]**

, SP-SEC-Serv-8-8 - The SCS-NAC shall use the SSI-IAM interface to check if the requesting Secure Component is authorized to access the network in the SCS-IAM. **[**SPPRAMSS-4944 **]**

, SP-SEC-Serv-8-9 - The SCS-NAC shall allow network access to a Secure Component, if the Secure Component is authorized based on its MDC and the asset exists in the SCS-IAM and its state is "COMMISSIONING". **[**SPPRAMSS-15433 **]**

, SP-SEC-Serv-8-10 - The SCS-NAC shall allow network access to a Secure Component, if the Secure Component is authorized based on the ODC and the asset exists in the SCS-IAM and its state is "ACTIVE". **[**SPPRAMSS-15432 **]**

, SP-SEC-Serv-8-11 - If the Secure Component is authorised to access the network, the SCS-NAC shall reply with a RADIUS EAP success to the RADIUS authenticator. **[**SPPRAMSS-4946 **]**

, SP-SEC-Serv-8-12 - If the Secure Component is not authorised to access the network, the SCS-NAC shall reply with a RADIUS EAP failure to the RADIUS authenticator. **[**SPPRAMSS-4947 **]**

, SP-SEC-Serv-8-13 - The Requirements for the Authenticator are defined in the Secure Component Specification in Chapter 5.4.3 of SP-SEC-Serv-2.3-29 - [SP-SEC-CompSpec]. **[**SPPRAMSS-4943 **]**

9 LOG: Security Logging

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

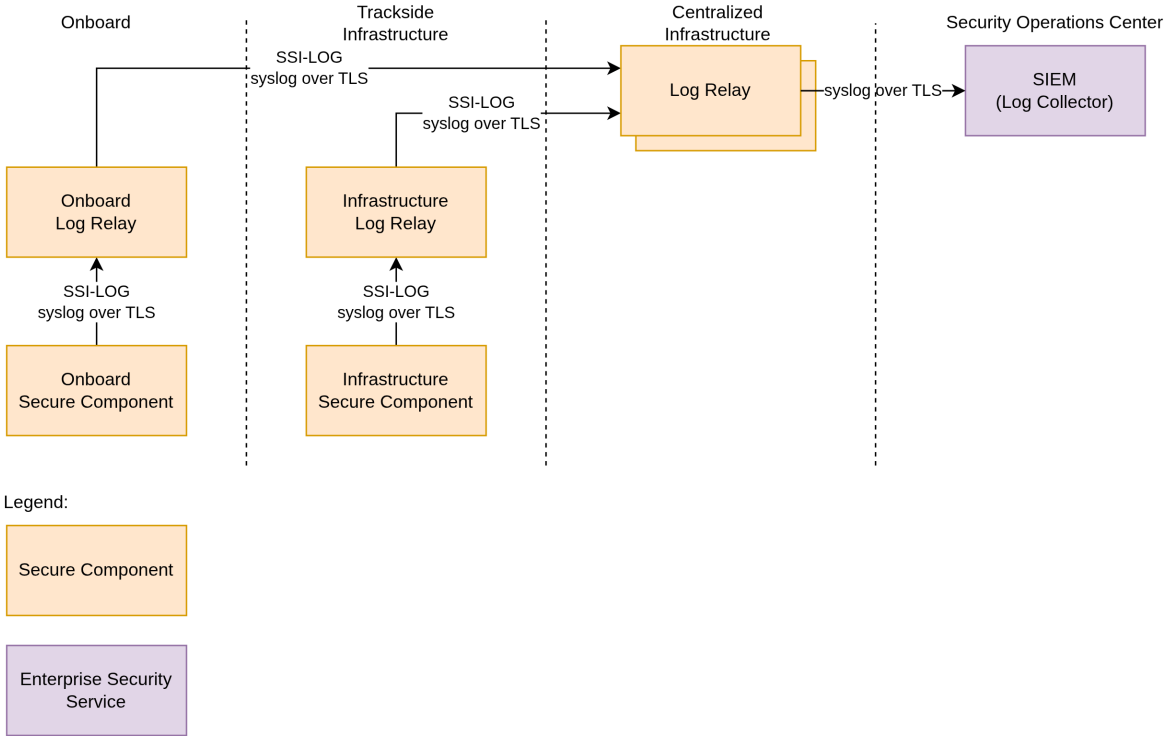

Figure 11 Exemplary Architecture of the Log Services

[SPPRAMSS-4786 **]**

, SP-SEC-Serv-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-Serv-9-5 - The communication partners using the SSI-LOG (Secure Component, log relay, log collector) shall use syslog over TLS as defined in RFC SP-SEC-Serv-2.3-11 - [RFC 5424] and SP-SEC-Serv-2.3-12 - [RFC 5425] for sending and/or receiving security log messages.
[SPPRAMSS-4404 **]**

, SP-SEC-Serv-9-6 - The communication partners using the SSI-LOG (Secure 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. **[**SPPRAMSS-12066 **]**

9.1 Log Message Format

9.1.1 Structured Data Format

, SP-SEC-Serv-9.1.1-1 - Log messages shall conform to the syslog format as defined in SP-SEC-Serv-2.3-11 - [RFC 5424]. **[**SPPRAMSS-4795 **]**

, SP-SEC-Serv-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 defined in Chapter 6.3 of SP-SEC-Serv-2.3-11 - [RFC 5424].
Note: This means, that 3rd party software (e.g. open source software) does not need be adapted. **[**SPPRAMSS-7522 **]**

, SP-SEC-Serv-9.1.1-3 - If a log message is not created by 3rd party software, the log message shall contain the SD-ID “SEC_LOG@” + vendor private enterprise number (see SP-SEC-Serv-2.3-2 - [IANA PENs]). **[**SPPRAMSS-4823 **]**

, SP-SEC-Serv-9.1.1-4 - If a log message is not created by 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.

Table 6 Log Structured Data fields

Keyword (PARAM-NAME as defined in [RFC 5424])	**Description**	**Allowed values** (PARAM-VALUE as defined in [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
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

Keyword (PARAM-NAME as defined in [RFC 5424])	**Description**	**Allowed values** (PARAM-VALUE as defined in [RFC 5424], additional values are allowed)	**Examples**
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
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	SSI_IAM_OPC_UA_MSG_13

[SPPRAMSS-4807 **]**

, 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

[SPPRAMSS-13915 **]**

9.1.2 Syslog Header Definitions

, SP-SEC-Serv-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-Serv-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-2.3-11 - [RFC 5424]. **[**SPPRAMSS-7976 **]**

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

, SP-SEC-Serv-9.1.2-4 - The 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). **[**SPPRAMSS-4806 **]**

, SP-SEC-Serv-9.1.2-5 - The 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). **[**SPPRAMSS-4804 **]**

, SP-SEC-Serv-9.1.2-6 - The 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-Serv-9.1.2-7 - The 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-Serv-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,	Unsuccessful changes CRL update failure first failed certificate update	System changes could affect security and availability repeated failed certificate update (one month before expiration)	System changes lead to a security and availability problems Changes of security configuration Factory reset repeated failed certificate update (two weeks before expiration)

Log Type	6 – Info	4 – Warning	3 – Error	1 – alert
	certificate revocations)			
Threat		Attack attempts and probes (e.g. pings, nmap scans, connection attempts, to 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 / 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

[SPPRAMSS-4803 **]**

, SP-SEC-Serv-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-Serv-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-2.3-11 - [RFC 5424] using UTC date/time format including milliseconds using TIME-SECFRAC.
Note: An Example for for such a timestamp is `2038-01-19T:03:14:08.000Z` **[**SPPRAMSS-4819 **]**

, SP-SEC-Serv-9.1.2-11 - The LOG originator shall set the HOSTNAME to one of the following values: FQDN, static IP address, hostname, dynamic IP address 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 **[**SPPRAMSS-4831 **]**

, SP-SEC-Serv-9.1.2-12 - The APP-NAME is a String containing the identification of the application that created the log message. **[**SPPRAMSS-4836 **]**

, SP-SEC-Serv-9.1.2-13 - Process ID of the syslog daemon is automatically set by syslog implementation. **[**SPPRAMSS-4834 **]**

, SP-SEC-Serv-9.1.2-14 - The LOG Originator shall set the MSGID as defined in SP-SEC-Serv-2.3-11 - [RFC 5424] to one of the following values:

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

[SPPRAMSS-4838 **]**

, SP-SEC-Serv-9.1.2-15 - The msg part of the syslog message is optional if the structured data contains all necessary information. **[**SPPRAMSS-4844 **]**

, SP-SEC-Serv-9.1.2-16 - If the msg part is used, the LOG originator shall use UNICODE with UTF-8 encoding. **[**SPPRAMSS-4843 **]**

, SP-SEC-Serv-9.1.2-17 - If the msg part is used, the LOG originator shall not use Octet values below 32 (control character range). **[**SPPRAMSS-4846 **]**

9.2 Log Message Examples

These examples showcase how log messages are structured:

- Authentication failure due to untrusted root certificate
```
<syslog header>[SEC_LOG@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 runtime integrity check failed
```
<syslog header>[SEC_LOG@32473 user="runtime-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_RUNTIME_INTEGRITY_MSG_1”]
```

- Secure Component Sending a Certificate Request

```
<syslog header>[SEC_LOG@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”]
```

10 UAS: User Authentication Service

, 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. **[**SPPRAMSS-12404 **]**

, SP-SEC-Serv-10-2 - The following UAS Endpoints exist

- SCS-UAS (OpenID Connect - Authorisation Server / OpenID Provider)
- UAS Client (OpenID Connect - Client Application & User Agent)
- UAS Resource Server (OpenID Connect - Resource Server)

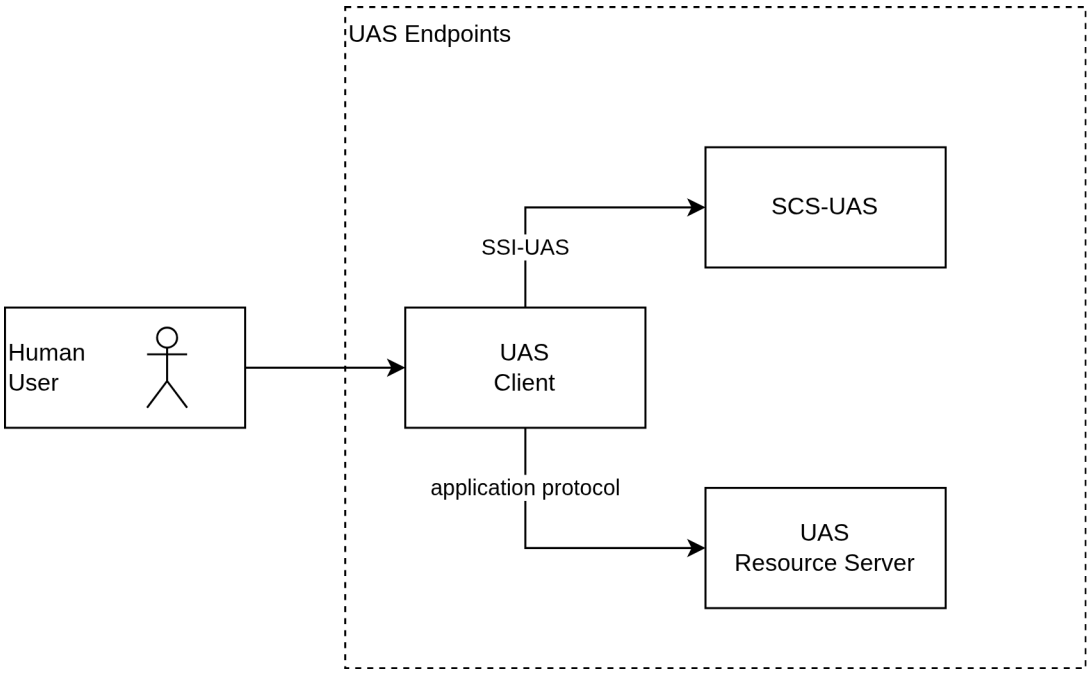

Figure 12 Endpoints of the User Authentication Service (UAS)

Note: UAS Client and Resource Server can be implemented in one or multiple Secure Components. **[**SPPRAMSS-16449 **]**

, SP-SEC-Serv-10-3 - The SCS-UAS shall support multi-factor authentication of human users. **[**SPPRAMSS-4675 **]**

, SP-SEC-Serv-10-4 - The UAS Resource Server shall only accept requests from human users authenticated via SCS-UAS. **[**SPPRAMSS-16451 **]**

, SP-SEC-Serv-10-5 - The UAS Resource Server shall only grant access to resources according to the token claims. **[**SPPRAMSS-16450 **]**

, SP-SEC-Serv-10-6 - The SSI-UAS Endpoint shall implement single sign-on (SSO) based on OpenID Connect 1.0 (OIDC) as defined in SP-SEC-Serv-2.3-4 - [OIDC 1.0]. **[**SPPRAMSS-6055 **]**

, SP-SEC-Serv-10-7 - The SSI-UAS Endpoint 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.
Note1: 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.
Note2: The use of PKCE as defined in SP-SEC-Serv-2.3-14 - [RFC 7636] is recommended. **[**SPPRAMSS-6066 **]**

, SP-SEC-Serv-10-8 - The SCS-UAS shall use an Operator Non-safety Communication Certificate (ONCC) for server authentication.
Note: SCS-UAS does not expect client authentication for the TLS connection **[**SPPRAMSS-15507 **]**

, SP-SEC-Serv-10-9 - The SCS-UAS shall support authentication with X.509 client certificates complying to the Operator User Certificate (OUC) profile see SP-SEC-Serv-14.1.2-4. **[**SPPRAMSS-6575 **]**

, SP-SEC-Serv-10-10 - The SCS-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-Serv-10-11 - The SCS-UAS should support passwordless authentication with at least one additional factor (e.g. passkeys with biometric factor). **[**SPPRAMSS-6576 **]**

10.1 SSI-Tokens for Authentication and Authorisation

, SP-SEC-Serv-10.1-1 - The SCS-UAS shall include in Access Tokens at least the JWT claims defined as mandatory according to SP-SEC-Serv-10.1-3 - JWT claims for Access Tokens and ID Tokens. **[**SPPRAMSS-6068 **]**

, SP-SEC-Serv-10.1-2 - The SSI-UAS shall include in ID Tokens at least the JWT claims defined as mandatory according to SP-SEC-Serv-10.1-3 - JWT claims for Access Tokens and ID Tokens. **[**SPPRAMSS-6559 **]**

, SP-SEC-Serv-10.1-3 - JWT claims for Access Tokens and ID Tokens

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 idle time at the service to be accessed (e.g. 30 minutes).	mandatory	mandatory

Claim	Description	Use in JWT access token	Use in JWT ID token
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-2.3-18 - [RFC 8176] • sc (Smartcard) plus pin (Personal Identification Number) • mfa (Multi-factor authentication), for example pwd (Password) plus otp (One-time Password) • A combination of hwk (hardware key) and swk (software key) plus fpt (fingerprint) and face (facial recognition)	mandatory	mandatory
email	email address of the authenticated user.	mandatory	mandatory

[SPPRAMSS-6578 **]**

, SP-SEC-Serv-10.1-4 - The SCS-UAS shall set the validity time of Access Tokens 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-Serv-10.1-5 - The SCS-UAS shall set the validity time of ID Tokens to a configurable maximum time. **[**SPPRAMSS-16452 **]**

10.2 Token Validation

, SP-SEC-Serv-10.2-1 - The SSI-UAS Resource Server shall verify the signature of a token before accepting it. **[**SPPRAMSS-6563 **]**

, SP-SEC-Serv-10.2-2 - The SSI-UAS Resource Server shall verify that all mandatory token claims as defined in SP-SEC-Serv-10.1-3 - JWT claims for Access Tokens and ID Tokens are included in the token. **[**SPPRAMSS-6580 **]**

, SP-SEC-Serv-10.2-3 - The SSI-UAS Resource Server shall verify the content of all included token claims **[**SPPRAMSS-6583 **]**

11 BKP: Backup and Restore

, SP-SEC-Serv-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.
  Note: MDM is defined in EULYNX Eu.Doc.18

[SPPRAMSS-9700 **]**

, SP-SEC-Serv-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-Serv-11-3 - Backup creation can be triggered locally (e.g. based on events or periodically) by a Secure Component. This backup is transferred via HTTPS POST to a preconfigured default URI. **[**SPPRAMSS-4538 **]**

, SP-SEC-Serv-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 SP-SEC-Serv-2.3-6 - [RFC 1952]
- `<YYYYMMDDThhmmssZ>_<secure-component-type>_<application-id>.metadata.json`: containing the backup metadata.

[SPPRAMSS-4486 **]**

, SP-SEC-Serv-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)
`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

Method Name	Description	Input Arguments	Output Arguments
			irrelevant)

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

, SP-SEC-Serv-11-6 - The SSI-BKP interface shall provide the the following OPC UA variables for report status information:

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	

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 **]**

12 MNT: Security Maintenance

, SP-SEC-Serv-12-1 - The following security maintenance method and diagnostic value definitions should be implemented using the protocols defined in SDI. **[**SPPRAMSS-12998 **]**

, SP-SEC-Serv-12-2 - The SSI-MNT server shall use an Operator Non-safety Communication Certificate (ONCC).
[SPPRAMSS-15509 **]**

, SP-SEC-Serv-12-3 - The SSI-MNT client shall use an Operator Non-safety Communication Certificate (ONCC).
[SPPRAMSS-15508 **]**

12.1 Overall Security Status

, 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. **[**SPPRAMSS-10127 **]**

, 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.
[SPPRAMSS-10126 **]**

12.2 Certificate Maintenance

, SP-SEC-Serv-12.2-1 - The SSI-MNT interface shall provide the maintenance method Security:UpdateCRLs() to request the update of the CRLs.
[SPPRAMSS-14139 **]**

, SP-SEC-Serv-12.2-2 - The SSI-MNT interface shall provide the maintenance method Security:RenewCert(in ByteString serialNumber, in String issuerDN) 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). **[**SPPRAMSS-4381 **]**

, SP-SEC-Serv-12.2-3 - The SSI-MNT interface shall provide the maintenance method Security:GetInstalledCerts(out File installedCertsFile) to obtain the public certificates available on the Secure Component.

Note: the output value installedCertsFile is a single PEM file containing all public certificates available on the Secure Component.
[SPPRAMSS-10138 **]**

, SP-SEC-Serv-12.2-4 - The SSI-MNT interface shall provide the maintenance method Security:GetInstalledTrustAnchors(out File installedTrustAnchorsFile) to obtain a list of installed trusted certificates.

Note: the output value installedTrustAnchorsFile is a single PEM file containing the installed and trusted certificates (trust anchors / root certificates / intermediate certificates). **[**SPPRAMSS-10139 **]**

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

Note: the output value installedCRLsFile is a GZIP compressed file containing all installed CRLs available on the Secure Component.
[SPPRAMSS-12393 **]**

12.3 Log Maintenance

, SP-SEC-Serv-12.3-1 - The SSI-MNT interface shall provide the maintenance method Security:GetSecurityLog(in Time startTime, in Time endTime, out File logFile) to access audit logs on a read-only basis for authorised humans and/or software processes.

Note: the return value is the content of the component log as a File object containing the logs from start time to end time.The SSI-MNT interface shall provide the diagnostic value Security:LogSize() (Uint64) to represent the size of the log in bytes.
[SPPRAMSS-10134 **]**

, SP-SEC-Serv-12.3-2 - The SSI-MNT interface shall provide the diagnostic value Security:GetLogSize(out Uint64 logSize) to represent the size of the log in bytes. **[**SPPRAMSS-15438 **]**

12.4 Configuration Management

, SP-SEC-Serv-12.4-1 - The SSI-MNT interface shall provide the maintenance method Security:GetComponentConfiguration(out String componentConfiguration) 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). **[**SPPRAMSS-10141 **]**

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

Note: this maintenance method can be used to detect changes in network configuration by comparing the result with previously stored configurations (or hashes). **[**SPPRAMSS-3088 **]**

12.5 Factory Reset

, SP-SEC-Serv-12.5-1 - The SSI-MNT interface shall provide the maintenance method Security:InitiateFactoryReset() to delete persistent data to reset the component to factory state.

Note 1: this method can be used as part of a decommissioning process SP-SEC-PrgmReq 9.2

Note 2: this method does not delete the factory key material (e.g. the MDC together with its root certificate will stay on the devices).

Note 3: this provides the user with the ability to erase data which requires confidentiality from persistent memory.

[SPPRAMSS-6748 **]**

12.6 Security Function Verification

, 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). **[**SPPRAMSS-10142 **]**

, SP-SEC-Serv-12.6-2 - The SSI-MNT interface shall provide the maintenance method Security:TestHostFirewall(in String destinationIPAddr, in UInt16 destinationPort, in String protocol) to test the functionality of the host-based firewall.

Note: a typical implementation is to have a process try to open a connection when this maintenance method is called to the destination address, port and protocol (either UDP or TCP) and then terminates. In case the connection is blocked by the host-based firewall, a log message is issued. This can be used to verify the security functionality of the host-based firewall.

[SPPRAMSS-10143 **]**

13 Security Requirements for DNS

, SP-SEC-Serv-13-1 - 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)

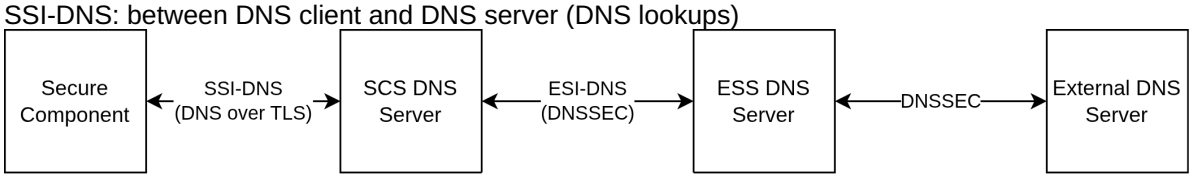

Figure 13 DNS Scope

Secure Components use DNS over TLS for DNS lookups. To reduce complexity, DNSSEC is not used by Secure Components.
Integrity of DNS records provided by ESS DNS servers or external DNS servers is ensured by using DNSSEC.
[SPPRAMSS-6652 **]**

, SP-SEC-Serv-13-2 - It is recommended that the SCS DNS server validates the DNS records provided by the higher DNS server using DNSSEC as defined in SP-SEC-Serv-2.3-24 - [RFC 9364].
[SPPRAMSS-8157 **]**

, SP-SEC-Serv-13-3 - The SCS-DNS server shall use DNS over TLS as defined in SP-SEC-Serv-2.3-17 - [RFC 7858]. **[**SPPRAMSS-5690 **]**

, SP-SEC-Serv-13-4 - The SCS-DNS server shall use an Operator Non-Safety Communication Certificates (ONCC). **[**SPPRAMSS-5693 **]**

, SP-SEC-Serv-13-5 - The SCS-DNS client shall use DNS over TLS as defined in SP-SEC-Serv-2.3-17 - [RFC 7858]. **[**SPPRAMSS-12407 **]**

, SP-SEC-Serv-13-6 - The SCS-DNS client shall use an Operator Non-Safety Communication Certificate (ONCC). **[**SPPRAMSS-15510 **]**

, SP-SEC-Serv-13-7 - DNS can be used to map CRL Distribution Points hosted by manufacturers to internal CRL Distribution Points hosted by operators (see SP-SEC-CompSpec Ch 5.5.2-9)
[SPPRAMSS-16306 **]**

14 Annex

14.1 Certificate Profiles

14.1.1 Manufacturer Certificate Profiles

, SP-SEC-Serv-14.1.1-1 - MDC

Table 10 Manufacturer Device Certificate (MDC) profile

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

Field Name	Content	Comment
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
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [manufacturer-specific cRLDistributionPoints]	

[SPPRAMSS-7641 **]**

, SP-SEC-Serv-14.1.1-2 - 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 issuing CA]	
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: 1.3.6.1.5.5.7.3.41
Subject Alternative Name	[manufacturer-specific]	optional
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [manufacturer-specific cRLDistributionPoints]	

[SPPRAMSS-7642]

, SP-SEC-Serv-14.1.1-3 - 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 issuing CA]	
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-trustAnchorConfigSigning	OID: 1.3.6.1.5.5.7.3.42
Subject Alternative Name	[manufacturer-specific]	optional
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [manufacturer-specific cRLDistributionPoints]	

[SPPRAMSS-7643]

, SP-SEC-Serv-14.1.1-4 - MUSC

Table 13 Manufacturer Update Signer Certificate (MUSC) profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of issuing CA]	
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-updatePackageSigning	OID: 1.3.6.1.5.5.7.3.43
Subject Alternative Name	[manufacturer-specific]	optional
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[manufacturer-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [manufacturer-specific cRLDistributionPoints]	

[SPPRAMSS-7644]

14.1.2 Operator Certificate Profiles

, SP-SEC-Serv-14.1.2-1 - 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
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 own 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
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific cRLDistributionPoints]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7648]

, SP-SEC-Serv-14.1.2-2 - 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]	recommended validity is 2 years
Subject	**mandatory:** CN=[use-case specific 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 OU shall be the ETCS ID type defined in [Subset-037-1] **other use cases:** CN shall be unique, e.g. 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)	**mandatory:** 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

Field Name	Content	Comment
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific cRLDistributionPoints]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7649 **]**

, SP-SEC-Serv-14.1.2-3 - 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 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 OU shall be the ETCS ID type defined in [Subset-037-1]. **EULYNX use case:** CN shall be unique, e.g. 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	OID: 1.3.6.1.5.5.7.3.44 serverAuth and/or clientAuth depending of the use case of the certificate
Subject Alternative Name	dNSName=[FQDN] iPAddress=[IP address]	either dNSName or iPAddress shall be used

Field Name	Content	Comment
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific cRLDistributionPoints]	distributionPoint contains URL to download CRLs within operator networ

[SPPRAMSS-7650 **]**

, SP-SEC-Serv-14.1.2-4 - OUC

Table 17 Table Operator User Certificate (OUC) 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 human user / software process] **recommended for human users:** surname=[last name of user] givenName=[first name of user] **recommended for all certificates:** O=[operator name] C=[operator country]	human 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]	
Subject Alternative Name	email=[email address of user]	email is an rfc822Name according to SP-SEC-Serv-2.3-10 - [RFC 5280] chapter 4.2.1.6
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted

Field Name	Content	Comment
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific cRLDistributionPoints]	distributionPoint contains URL to download CRLs within operator network

[SPPRAMSS-7651 **]**

, SP-SEC-Serv-14.1.2-5 - OCSC

Table 18 Operator Configuration Signer Certificate (OCSC) 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 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], 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: 1.3.6.1.5.5.7.3.41
Subject Alternative Name	[operator-specific]	optional
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted

Field Name	Content	Comment
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific cRLDistributionPoints]	

[SPPRAMSS-7653 **]**

, SP-SEC-Serv-14.1.2-6 -

Table 19 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 issuing CA]	
Validity	[operator-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 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)	digitalSignature	
Extended Key Usage (critical)	id-kp-trustanchorConfigSigning	OID: 1.3.6.1.5.5.7.3.42
Subject Alternative Name	[operator-specific]	optional
Basic Constraints (critical)	**mandatory:** CA:FALSE	Required for all end-entity certificates; pathLenConstraint omitted
Certificate Policies	[operator-defined policy information]	optional, if used, content shall comply to SP-SEC-Serv-2.3-10 - [RFC 5280]
CRL Distribution Points	**mandatory:** [operator-specific cRLDistributionPoints]	

[SPPRAMSS-9942 **]**

14.1.3 CA Certificate Profiles

, SP-SEC-Serv-14.1.3-1 -

Table 20 CA Certificate profile

Field Name	Content	Comment
Version	0x2	X.509 v3
Serial Number	[integer]	
Signature Algorithm	SHA512withECDSA	
Issuer	[Subject DN of issuing CA]	
Validity	[manufacturer/operator-specific period]	recommended validity period is 15 years for self-signed operator (root) CAs recommended validity period is 5 years for operator intermediate CAs
Subject	[manufacturer/operator-specific]	
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)	keyCertSign cRLSign	Additional key usages are allowed to enable additional use cases.
Subject Alternative Name	[manufacturer/operator-specific]	optional
Certificate Policies	[manufacturer/operator-defined policy information]	optional
Basic Constraints (critical)	cA: true pathLenConstraint: [optional]	
CRL Distribution Points	[manufacturer/operator-specific distributionPoint]	optional for self-signed (root) CAs required for intermediate CAs

[SPPRAMSS-16108 **]**