EU-RAIL SYSTEM PILLAR

# Secure Communication Specification

**Version: 1.1.1**

# Secure Communication Specification

## Document data

| | |
|---|---|
| Created by | System Pillar Cybersecurity Domain |
| Classification | Public |
| Status | Released |
| Version | 1.1.1 |
| Date | 28-OCT-2026 |

## Copyright

© Europe's Rail Joint Undertaking, 2026

This document is drafted by and belongs to EU Rail.

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

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

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

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

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

## Document History

| Version | Date | Description | Status |
|---|---|---|---|
| 1.1.1 | 28-OCT-2026 | Release for ERA Technical Documents | released |
| 1.1 | 23-MAR-2026 | Error correction and additional guidance for version 1.0 | released |
| 1.0 | 20-FEB-2025 | Initial public release | released |

## 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

# 1 Table of Contents

1 Table of Contents . . . . . 4
2 Preamble . . . . . 5
2.1 Scope, Purpose and Intended Audience . . . . . 5
2.2 Document Usage . . . . . 5
2.3 References . . . . . 5
2.4 Terms and Definitions . . . . . 6
2.5 Abbreviation list . . . . . 7
3 End-to-End Security Layer (TLS) . . . . . 7
3.1 TLS Overall . . . . . 7
3.2 TLS Requirements for TLS-PKI . . . . . 7
3.3 Error Reporting for Diagnostic Purpose . . . . . 8
4 Secure Communication for OPC UA . . . . . 8
5 Secure Communication for HTTP . . . . . 10
6 PKI certificate validation for Communication Endpoints . . . . . 11

# 2 Preamble

## 2.1 Scope, Purpose and Intended Audience

**, SP-SEC-Comm-2.1-1 -** This specification is a toolkit to harmonise interoperability-related cybersecurity requirements for communication protocols. **[**SPPRAMSS-3780 **]**

**, SP-SEC-Comm-2.1-2 -** The documents defining a communication interface (e.g. TSI CCS Subset-154 or other TSIs) specify the applicable requirements of this document by referring to the relevant chapters. **[**SPPRAMSS-18524 **]**

**, SP-SEC-Comm-2.1-3 -** The requirements in this document require cybersecurity services defined in Shared Cybersecurity Services Specification. **[**SPPRAMSS-18522 **]**

**, SP-SEC-Comm-2.1-4 -** This document is intended for authors of communication and interface specifications in the rail domain (e.g. Subset specifications), as well as product developers, cybersecurity experts, system designers, and system architects. **[**SPPRAMSS-18523 **]**

## 2.2 Document Usage

**, SP-SEC-Comm-2.2-1 -** This specification uses identifiers starting with "SP-SEC-Comm". **[**SPPRAMSS-14016 **]**

**, SP-SEC-Comm-2.2-2 -** Icon types used in this document are defined in SP-SEC-Tax. **[**SPPRAMSS-14015 **]**

**, SP-SEC-Comm-2.2-3 -** For a definition of the words "shall", "should" and "may" used in this specification, refer to SP-SEC-Comm-2.3-4 - [ISO/IEC Directives, Part 2] . **[**SPPRAMSS-18559 **]**

## 2.3 References

**, SP-SEC-Comm-2.3-1 -** This chapter contains all references of this document. For a complete list including external references see [SP-SEC-Tax] Chapter 3. **[**SPPRAMSS-14017 **]**

**[SP-SEC-ServSpec]**
Europe's Rail System Pillar Cybersecurity Domain - Shared Cybersecurity Services Interface Specification, v1.1

**[SP-SEC-Tax]**
Europe's Rail System Pillar Cybersecurity Domain - Taxonomy and References, v1.1

**[ISO/IEC Directives, Part 2]**
Principles and rules for the structure and drafting of ISO and IEC documents

**[RFC 4086]**
Randomness Requirements for Security

**[RFC 5280]**
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

**[RFC 8446]**
The Transport Layer Security (TLS) Protocol Version 1.3.

**[RFC 9150]**
TLS 1.3 Authentication and Integrity-Only Cipher Suites

**[OPC UA-10000-4]**
OPC 10000-4 (Release 1.05.07): UA Part 4: Services

**[OPC UA-10000-6]**
OPC 10000-6 (Release 1.05.07): UA Part 6: Mappings

**[OPC UA - SecurityPolicy – ECC-nistP256-ChaChaPoly]**
UACore 1.05

**[OPC UA - SecurityPolicy – ECC-nistP384-AesGcm]**
UACore 1.05

**[OPC UA Profile SecurityPolicy [B] – Basic256Sha256]**
SecurityPolicy [B] – Basic256Sha256

## 2.4 Terms and Definitions

**- Communication endpoint**
A communication endpoint is a software process exposing or using a communication protocol, including but not limited to TLS, OPC UA, HTTP or other communication protocols.

**- TLS endpoint**
A TLS endpoint is a Secure Component using TLS-protected communication (client and server).

**- OPC UA endpoint**
An OPC UA endpoint is a Secure Component using OPC UA communication (client and server).

**- HTTP endpoint**
An HTTP endpoint is a Secure Component using HTTP communication (client and server).

### 2.5 Abbreviation list

All abbreviation are listed in [SP-SEC-Tax] document.

## 3 End-to-End Security Layer (TLS)

**, SP-SEC-Comm-3-1 -** Note: This chapter applies to communication that uses TLS. **[**SPPRAMSS-7358 **]**

**, SP-SEC-Comm-3-2 -** Note: This chapter does not cover backwards compatibility. As a result there are no specifications for migration from older or outdated TLS versions to the currently specified TLS version. **[**SPPRAMSS-2419 **]**

### 3.1 TLS Overall

**, SP-SEC-Comm-3.1-1 -** The TLS endpoint shall use TLS version 1.3 as defined in SP-SEC-Comm-2.3-7 - [RFC 8446]. **[**SPPRAMSS-1713 **]**

**, SP-SEC-Comm-3.1-2 -** The TLS endpoint shall not use the 0-RTT mode. **[**SPPRAMSS-1716 **]**

**, SP-SEC-Comm-3.1-3 -** The TLS endpoint shall enforce mutual authentication. **[**SPPRAMSS-1954 **]**

**, SP-SEC-Comm-3.1-4 -** Implementation and initialisation of the random number generator shall follow Appendix C.1 in SP-SEC-Comm-2.3-7 - [RFC 8446] .
Note: As mentioned in the appendix C.1, additional guidance on the generation of random values is provided by SP-SEC-Comm-2.3-5 - [RFC 4086] . **[**SPPRAMSS-3036 **]**

**, SP-SEC-Comm-3.1-5 -** The TLS endpoint shall support the cipher TLS_AES_256_GCM_SHA384. **[**SPPRAMSS-1959 **]**

**, SP-SEC-Comm-3.1-6 -** The TLS endpoint shall support the cipher TLS_CHACHA20_POLY1305_SHA256. **[**SPPRAMSS-1960 **]**

**, SP-SEC-Comm-3.1-7 -** If only integrity protection is required, the TLS endpoint shall support the cipher TLS_SHA384_SHA384. SP-SEC-Comm-2.3-8 - [RFC 9150]
Note: Integrity-only protection can be used for Automatic Train Operation [Subset-148], Automatic Train Protection [Subset-037-3], and EULYNX SCI [Eu.Doc.92]. **[**SPPRAMSS-1961 **]**

**, SP-SEC-Comm-3.1-8 -** The TLS server shall reject ciphers not defined in this specification. **[**SPPRAMSS-15422 **]**

**, SP-SEC-Comm-3.1-9 -** In future version of this document, the ciphers for securing communication will be extended to support additional ciphers, e.g. for post quantum cryptography (PQC). **[**SPPRAMSS-10108 **]**

**, SP-SEC-Comm-3.1-10 -** If the Pre-Shared Key extension is used, the TLS server shall reject TLS connection establishment. **[**SPPRAMSS-18601 **]**

### 3.2 TLS Requirements for TLS-PKI

**, SP-SEC-Comm-3.2-1 -** The TLS endpoint shall perform authentication using certificates in accordance with X.509 (SP-SEC-Comm-2.3-6 - [RFC 5280]). **[**SPPRAMSS-2030 **]**

**, SP-SEC-Comm-3.2-2 -** The TLS endpoint shall validate peer certificates according to chapter 6 - PKI certificate validation for Communication Endpoints. **[**SPPRAMSS-18648 **]**

**, SP-SEC-Comm-3.2-3 -** If DNS resolution was used to resolve the IP address for the corresponding connection, the TLS endpoint shall abort the connection if the DNS FQDN does not match the dNSName in the Subject Alternative Name of the communication partners certificate. **[**SPPRAMSS-12360 **]**

**, SP-SEC-Comm-3.2-4 -** If DNS resolution was not used to resolve the IP address for the corresponding connection, the TLS endpoint shall abort the connection if the IP address does not match the iPAddress in the Subject Alternative Name of the communication partners certificate. **[**SPPRAMSS-12359 **]**

**, SP-SEC-Comm-3.2-5 -** If a Common Name is used to identify the communication partner, the TLS endpoint shall abort the connection if the expected Common Name does not match the Common Name of the communication partners certificate.
Note: This procedure is used e.g. for EULYNX SCI connections. **[**SPPRAMSS-12357 **]**

### 3.3 Error Reporting for Diagnostic Purpose

**, SP-SEC-Comm-3.3-1 -** The TLS endpoint shall log the events reported by the TLS implementation via SSI-LOG defined in Shared Cybersecurity Services Specification Chapter 9 LOG: Security Logging.
Note: Fatal TLS 1.3 errors are defined in SP-SEC-Comm-2.3-7 - [RFC 8446], Chapter 6.2.
**[**SPPRAMSS-5857 **]**

## 4 Secure Communication for OPC UA

**, SP-SEC-Comm-4-1 -** Note: This chapter applies to communication that uses OPC UA. **[**SPPRAMSS-7357 **]**

**, SP-SEC-Comm-4-2 -** The OPC UA endpoint shall use Secure Conversation (UASC) (SP-SEC-Comm-2.3-10 - [OPC UA-10000-6] , Chapter 6.7) **[**SPPRAMSS-2952 **]**

**, SP-SEC-Comm-4-3 -** The OPC UA endpoint shall use SignAndEncrypt as security mode. **[**SPPRAMSS-2953 **]**

**, SP-SEC-Comm-4-4 -** The OPC UA endpoint shall use mutual authentication via certificates.
Note: OPC UA certificate validation is defined in SP-SEC-Comm-2.3-9 - [OPC UA-10000-4] Chapter 6.1.3
**[**SPPRAMSS-2951 **]**

**, SP-SEC-Comm-4-5 -** The OPC UA SC endpoint shall validate peer certificates according to chapter 6 - PKI certificate validation for Communication Endpoints.
**[**SPPRAMSS-18649 **]**

**, SP-SEC-Comm-4-6 -** If an URI is used to uniquely identify the communication partners application, the OPC UA endpoint shall abort the connection if the expected URI does not match the URI in the Subject Alternative Name of the communication partners certificate. **[**SPPRAMSS-12358 **]**

**, SP-SEC-Comm-4-7 -** The OPC UA endpoint shall enforce the permissions attached to each node of the OPC-UA model. **[**SPPRAMSS-4951 **]**

**, SP-SEC-Comm-4-8 -** The OPC UA endpoint shall support the following Security Policies defined in UACore 1.05:

- ECC-nistP256-ChaChaPoly (SP-SEC-Comm-2.3-11 - [OPC UA - SecurityPolicy – ECC-nistP256-ChaChaPoly])
- ECC-nistP256-AesGcm (SP-SEC-Comm-2.3-12 - [OPC UA - SecurityPolicy – ECC-nistP384-AesGcm] )

**[**SPPRAMSS-7325 **]**

**, SP-SEC-Comm-4-9 -** The OPC UA server shall reject Security Policies not defined in this specification. **[**SPPRAMSS-15423 **]**

**, SP-SEC-Comm-4-10 -** The OPC UA endpoint may support the Security Policy SP-SEC-Comm-2.3-13 - [OPC UA Profile SecurityPolicy [B] – Basic256Sha256]

Note: The preferred Security Policies are the ones using Elliptic Curve Cryptography (ECC). RSA can only be used for backwards compatibility implementations which do not support ECC yet. Support for RSA will be removed in a future version of this specification. **[**SPPRAMSS-13068 **]**

**, SP-SEC-Comm-4-11 -** The OPC UA endpoint shall support the following permissions:

| Permission Name | Description | Corresponding OPC UA Permissions |
|---|---|---|
| `eu.rail.ssi.security-read` | Permission to retrieve security-related properties via SSI-MNT. | `Browse`<br>`Read`<br>`ReceiveEvents`<br>`Call` |
| `eu.rail.ssi.security-execute` | Permission to change security-related properties via SSI-MNT (e.g. certificate management). | `Browse`<br>`Read`<br>`ReceiveEvents`<br>`Call` |
| `eu.rail.ssi.security-test` | Permission to execute security-related tests (e.g. testing host firewall functionality) via SSI-MNT. | `Browse`<br>`Read`<br>`ReceiveEvents`<br>`Call` |
| `eu.rail.ssi.factory-reset` | Permission to perform a factory-reset via SSI-MNT. | `Browse`<br>`Read`<br>`ReceiveEvents`<br>`Call` |

| | | |
|---|---|---|
| `eu.rail.ssi.backup-create` | Permission to create backups via SSI-BKP. | `Browse`<br>`Read`<br>`ReceiveEvents`<br>`Call` |
| `eu.rail.ssi.backup-restore` | Permission to restore backups via SSI-BKP. | `Browse`<br>`Read`<br>`ReceiveEvents`<br>`Call` |

**[**SPPRAMSS-8867 **]**

**, SP-SEC-Comm-4-12 -** If additional permissions are required, they should be defined using the following pattern:
`[tld].[organisation].[interface].[permission name]`
where `[permission name]` should have a clear semantic meaning that a human user understands.

For example:
`com.company.smi.manufacturer-execute` **[**SPPRAMSS-8868 **]**

**, SP-SEC-Comm-4-13 -** The OPC UA endpoint shall enforce permissions retrieved via the SSI-IAM interface. **[**SPPRAMSS-9756 **]**

**, SP-SEC-Comm-4-14 -** If the OPC UA endpoint cannot retrieve the permissions, the OPC UA endpoint shall deny access to OPC UA nodes requiring permissions. **[**SPPRAMSS-18520 **]**

**, SP-SEC-Comm-4-15 -** The OPC UA server and client shall use an Operator User Certificate (OUC as defined in Shared Cybersecurity Services Specification 14.1.2-4) for OPC UA session application layer authentication. **[**SPPRAMSS-16316 **]**

**, SP-SEC-Comm-4-16 -** The OPC UA server and client shall use an Operator Non-safety Communication Certificate (ONCC as defined in Shared Cybersecurity Services Specification 14.1.2-2) for OPC UA session communication layer authentication.
Note: OPC UA is used for non-safety related communication only. **[**SPPRAMSS-16315 **]**

## 5 Secure Communication for HTTP

**, SP-SEC-Comm-5-1 -** The HTTP endpoint shall use TLS for HTTP communication according to 2.5 - Abbreviation list. **[**SPPRAMSS-8864 **]**

**, SP-SEC-Comm-5-2 -** HTTP communication without TLS is allowed for SSI-PKI (for CRL download and CMP over HTTP) as defined in Shared Cybersecurity Services Specification Chapter 6 PKI: Public Key Infrastructure. **[**SPPRAMSS-10322 **]**

**, SP-SEC-Comm-5-3 -** Requirements for human user authorization in HTTP communication are defined by the corresponding interface specification (Shared Cybersecurity Services Specification Chapter 10 UAS : User Authentication Service). **[**SPPRAMSS-11959 **]**

# 6 PKI certificate validation for Communication Endpoints

**, SP-SEC-Comm-6-1 -** The communication endpoint using certificate-based authentication shall validate certificates according to X.509 as defined in [RFC 5280] Chapter 6.
Note: the RFC 5280 defines the validation of the certificate's trust chain up to a trusted certificate authority and how to check the certificate validity periods in the certificate path. **[**SPPRAMSS-18636 **]**

**, SP-SEC-Comm-6-2 -** The communication endpoint shall validate the certificate algorithms, key lengths, profile, Key Usage and Extended Key Usage according to the definition in Shared Cybersecurity Services Specification Chapter 14.1 Certificate Profiles. **[**SPPRAMSS-18638 **]**

**, SP-SEC-Comm-6-3 -** The communication endpoint shall establish that the communication partner controls the private key corresponding to the public key contained in the authenticated certificate.
Note: this requirement is fulfilled by TLS and OPC UA SC specifications and implementations. **[**SPPRAMSS-18646 **]**

**, SP-SEC-Comm-6-4 -** The communication endpoint shall map the authenticated identity of a certificate to a device, software process, technical user or human user, depending on the communication use case.
Note: The mapped identity is to be used for authorization decisions. **[**SPPRAMSS-18637 **]**

**, SP-SEC-Comm-6-5 -** If the communication endpoint cannot validate certificates because of a missing secure time source (e.g. during initial commissioning), the communication endpoint shall use a fallback time source.
Note: The fallback time can for example be calculated using the following (possibly non-secure) time sources: NTP, last shutdown time, real-time clock of the device. **[**SPPRAMSS-18642 **]**

**, SP-SEC-Comm-6-6 -** The communication endpoint shall check the revocation status of each certificate in the certificate path using Certificate Revocation Lists according to [RFC 5280] Chapter 6.3.
Note: Self-signed certificates (e.g. trust anchors) do not have a revocation status which can be validated.
RFC 5280 defines checks for the following conditions:

- the CRL signature is valid;
- the CRL issuer is the expected certificate authority;
- the CRL can be linked to the certificate issuer;
- the current time is within the CRL validity period;
- the current time is earlier than or equal to the CRL nextUpdate value;
- the CRL applies to the certificate being validate

**[**SPPRAMSS-18639 **]**

**, SP-SEC-Comm-6-7 -** If the status of a certificate is revoked or no valid certificate revocation information is available, the communication endpoint shall abort the connection setup.
Note: no valid certificate revocation information is available when the current time is after the nextUpdate field and a new CRL can not be fetched. **[**SPPRAMSS-2427 **]**

**, SP-SEC-Comm-6-8 -** If the communication endpoint cannot fetch a new CRL, the communication endpoint shall issue a log message. **[**SPPRAMSS-18691 **]**

**, SP-SEC-Comm-6-9 -** If certificate validation fails for any reason, including invalid signature, untrusted certificate path, expired certificate, revoked certificate, inappropriate certificate usage, unsupported cryptographic algorithm, or non-control of the private key, the communication endpoint shall reject the

certificate.
Note: If the certificate is required for connection establishment, the communication endpoint will abort the connection setup.
**[**SPPRAMSS-18647**]**

**, SP-SEC-Comm-6-10 -** For non-safety-related communication, the communication endpoint shall use and accept Operator Non-Safety Communication Certificates (ONCC as defined in Shared Cybersecurity Services Specification 14.1.2-2). **[**SPPRAMSS-8869**]**

**, SP-SEC-Comm-6-11 -** For safety-related communication, the communication endpoint shall use and accept Operator Safety Communication Certificates (OSCC as defined in Shared Cybersecurity Services Specification 14.1.2-3 ). **[**SPPRAMSS-8870**]**