

# Secure Communication Specification

---

## Disclaimer

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

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

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models 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 trademarks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

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

## Maintenance

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


[cybersecurity.review@ertms.be](mailto:cybersecurity.review@ertms.be)

## 1 Table of Contents


1	Table of Contents	2
2	Preamble	3
2.1	Scope, Purpose and Intended Audience	3
2.2	Document Usage	3
2.3	References	3
2.4	Terms and Definitions	4
2.5	Modification History	4
3	End-to-End Security Layer (TLS)	5
3.1	TLS Overall	5
3.2	TLS Requirements for TLS-PKI	6
3.3	Error Reporting for Diagnostic Purpose	7
4	Secure Communication for OPC UA	7
5	Secure Communication for HTTP	8
6	Securing other Communicating Interfaces	9
6.1	Identification, Authentication and Authorization	9
6.2	Communication Integrity and Confidentiality	10
6.3	Access Logging	10
6.4	DoS Resilience and Minimising Negative Impact	10


## 2 Preamble

### 2.1 Scope, Purpose and Intended Audience


 , **SP-SEC-Comm-2.1-1** - This specification is a Functional Interface Specification (FIS) for the security layer of Secure Components required for interoperability.

### 2.2 Document Usage

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

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

### 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.

#### **[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-10000-6]**

OPC 10000-6: UA Part 6: Mappings

#### **[OPC UA Profile SecurityPolicy [ECC-B] – ECC-nistP256]**

Profile SecurityPolicy [ECC-B] – ECC-nistP256

#### **[OPC UA Profile SecurityPolicy – ECC-brainpoolP256r1]**

Profile SecurityPolicy – ECC-brainpoolP256r1

#### **SP-SEC-Comm-2.3-9 - [OPC UA Profile SecurityPolicy [B] – Basic256Sha256]**

SecurityPolicy [B] – Basic256Sha256

#### **[OPC UA-10001-4 Amendment 4: ECC]**

ECC for UACore 1.04

## 2.4 Terms and Definitions

### - TLS endpoint

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

### - OPC UA endpoint

The OPC UA endpoint is a Secure Component using OPC UA communication (client and server).

### - HTTP endpoint


The HTTP endpoint is a Secure Component using HTTP communication (client and server).


## 2.5 Modification History

First release (V1.0) - February 2025


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


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

 , **SP-SEC-Comm-3-1** - Note: This chapter applies to all communication that uses TLS.


 , **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.

#### 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-2.3-4 - [RFC 8446].

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


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

**SP-SEC-Comm-3.1-4**,  - Implementation and initialisation of the random number generator shall follow the recommendations given by Appendix C.1 in SP-SEC-Comm-2.3-4 - [RFC 8446] .


Note: As mentioned in the appendix C.1, additional guidance on the generation of random values is provided by SP-SEC-Comm-2.3-2 - [RFC 4086] .

**SP-SEC-Comm-3.1-5**,  - The TLS endpoint shall support the cipher TLS\_AES\_256\_GCM\_SHA384.


Note: This cipher is preferred.

**SP-SEC-Comm-3.1-6**,  - The TLS endpoint shall support the cipher TLS\_CHACHA20\_POLY1305\_SHA256.


Note: This cipher is lower prioritized.


**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-2.3-5 - [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].


 , **SP-SEC-Comm-3.1-8** - Note: 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).


### 3.2 TLS Requirements for TLS-PKI


**SP-SEC-Comm-3.2-1,**  - The TLS endpoint shall perform authentication using certificates in accordance with [SP-SEC-Serv-6.3-2](#).


**SP-SEC-Comm-3.2-2,**  - The TLS endpoint shall send the certificate chain when initiating a TLS handshake.

Note: According to [SP-SEC-Comm-2.3-4](#) - [RFC 8446] the trust anchor MAY be omitted from the chain, provided that supported peers are known to possess any omitted certificates.


**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 expected DNS FQDN does not match the `dNSName` in the Subject Alternative Name of the communication partners certificate.

**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 expected IP address does not match the `iPAddress` in the Subject Alternative Name of the communication partners certificate.


**SP-SEC-Comm-3.2-5,**  - If an URI is used to uniquely identify the communication partners application, the TLS endpoint shall abort the connection if the expected URI does not match the URI in the Subject Alternative Name of the communication partners certificate.


**SP-SEC-Comm-3.2-6,**  - If an strongly typed Common Name which is not part of the Subject Alternative 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 for EULYNX SCI connections.

**SP-SEC-Comm-3.2-7,**  - The TLS endpoint shall check the certificate revocation status using Certificate Revocation Lists (CRLs) according to [SP-SEC-Comm-2.3-3](#) - [RFC 5280] (Chapter 6.1.3.).

Note: This includes checking the certificate revocation status using CRLs of all certificates in the certificate path (excluding self-signed trust anchors).


**SP-SEC-Comm-3.2-8,**  - If the status of a certificate is revoked or no valid certificate revocation information is available, the TLS endpoint shall abort the connection setup.

**SP-SEC-Comm-3.2-9,**  - The TLS endpoint shall re-validate the communication partner's certificate including the revocation status at least every 24 hours.


**SP-SEC-Comm-3.2-10,**  - If the re-validation of a certificate fails, the TLS endpoint shall terminate the TLS connection.

**SP-SEC-Comm-3.2-11,**  - If the TLS communication is not safety-related, the TLS endpoint shall

use an ONCC as defined in [SP-SEC-Serv-14.1.2-2](#)

**SP-SEC-Comm-3.2-12**,  - If the TLS communication is safety-related, the TLS endpoint shall use an OSCC as defined in [SP-SEC-Serv-14.1.2-3](#)


### 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.

Note: Fatal TLS 1.3 errors are defined in [SP-SEC-Comm-2.3-4 - \[RFC 8446\]](#), Chapter 6.2.


## 4 Secure Communication for OPC UA


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

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


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

**SP-SEC-Comm-4-4**,  - The OPC UA endpoint shall use mutual authentication via certificates.


**SP-SEC-Comm-4-5**,  - The OPC UA endpoint shall enforce the permissions attached to each node of the OPC-UA model.

**SP-SEC-Comm-4-6**,  - The OPC UA endpoint shall support the Security Policy ECC-nistP256.

Note: This Security Policy is defined in Amendment 4: ECC for UACore 1.04 [SP-SEC-Comm-2.3-10 - \[OPC UA-10001-4 Amendment 4: ECC\]](#) and in UACore 1.05 [SP-SEC-Comm-2.3-7 - \[OPC UA Profile SecurityPolicy \[ECC-B\] – ECC-nistP256\]](#)

**SP-SEC-Comm-4-7**,  - The OPC UA endpoint shall support the Security Policy ECC-brainpoolP256r1

Note: This Security Policy is defined in Amendment 4: ECC for UACore 1.04 [SP-SEC-Comm-2.3-10 - \[OPC UA-10001-4 Amendment 4: ECC\]](#) and in UACore 1.05 [SP-SEC-Comm-2.3-8 - \[OPC UA Profile SecurityPolicy – ECC-brainpoolP256r1\]](#).


, **SP-SEC-Comm-4-8** - The OPC UA endpoint may support the Security Policy [SP-SEC-Comm-2.3-9 - \[OPC UA Profile SecurityPolicy \[B\] – Basic256Sha256\]](#)

Note: The preferred Security Policies are the ones using Elliptic Curve Cryptography (ECC). Support for RSA may be required for backwards compatibility implementations which do not support ECC yet. RSA will be removed in a future version of this specification.

**SP-SEC-Comm-4-9**,  - The OPC UA endpoint shall support the following permissions:

Permission Name	Description	Corresponding OPC UA Permissions (Browse, Read, Execute, ReceiveEvents)

Permission Name	Description	Corresponding OPC UA Permissions (Browse, Read, Execute, ReceiveEvents)
eu.rail.ssi.security-read	Permission to read OPC UA nodes containing security-related information.	Browse Read ReceiveEvents
eu.rail.ssi.security-execute	Permission to execute OPC UA methods to execute security-related methods.	Browse Execute


 **SP-SEC-Comm-4-10** - 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
```

 **SP-SEC-Comm-4-11** - The permissions are retrieved via the SSI-IAM interface and enforced by the Secure Component. (see [SP-SEC-Comp-7.2-2](#) )

## 5 Secure Communication for HTTP

**SP-SEC-Comm-5-1**,  - The HTTP endpoint shall use TLS for HTTP communication according to 3 - End-to-End Security Layer (TLS).

 **SP-SEC-Comm-5-2** - Exceptions for the usage of TLS for HTTP communication are defined in the Shared Cybersecurity Services Specification.

 **SP-SEC-Comm-5-3** - Requirements for human user authorization in HTTP communication are defined by the corresponding interface specification. (SP-SEC-SERV User Authentication Service)



## 6 Securing other Communicating Interfaces

This chapter contains requirements for additional communication interfaces using other communication protocols which are not defined in this specification. These requirements are required to achieve compliance to EU CRA and IEC 62443-4-2.

Examples of other communication interfaces: SSH, FTPS,...


In general, all maintenance and diagnostic activities should be conducted using existing interfaces (e.g. SDI, SMI,...).

Direct access to the operating system is not advisable and should be avoided.


As per EU-CRA and IEC 62443-4-2, the attack surface of a device is required to be limited. Therefore, additional communication interfaces should only be added, if there are essential for the operation and can not be avoided. See corresponding [SP-SEC-CompSpec Ch 5.3.6 - Hardening](#) for corresponding requirements.

If specific other communication protocols are used extensively, this specification can be extended to define a security profile for the specific protocol to allow interoperability between communications partners.


### 6.1 Identification, Authentication and Authorization

**SP-SEC-Comm-6.1-1**,  - Each software process realizing an additional communication interface shall be capable of identifying itself and authenticate to any other communication partner using a unique X.509 v3 certificate as defined in [SP-SEC-Comm-2.3-3 - \[RFC 5280\]](#).

Note: a certificate should identify a software process (web server, safety communication, diagnostic server,...), not per software process instance of the same software process.


**SP-SEC-Comm-6.1-2**,  - Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity.

Note: in case of certificate-based identification, see checks in chapter [SP-SEC-CompSpec-5.5.3 - PKI certificate validation](#). In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable.

**SP-SEC-Comm-6.1-3**,  - Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization.


Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH, ...), but not applicable for safety-relevant communication / M2M communication.

Note2: in case of non-availability of the IAM, local accounts can be used


**SP-SEC-Comm-6.1-4**,  - Each software process realizing an additional communication interface shall enforce access based on retrieved permissions.

Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component.

## 6.2 Communication Integrity and Confidentiality

**SP-SEC-Comm-6.2-1**,  - Each software process realizing an additional communication interface shall protect the integrity of data in transit.


Note: this should, if applicable, be realized preferable using TLS with an integrity cipher. In any case, a cryptographic method for integrity protection is required

**SP-SEC-Comm-6.2-2**,  - If data in transit is considered confidential, a software process realizing an additional communication interface shall provide the capability to protect the confidentiality of data in transit.


Note: this should, if applicable, be realized preferable using TLS with an encryption cipher.

Examples of confidential data in transit are encryption keys, legally protected personal data, user credentials, person/user related data, financial information, security related logs and/or diagnosis data.


## 6.3 Access Logging

 , **SP-SEC-Comm-6.3-1** - Security logging for communication interface accesses is required by EU CRA and IEC 62443-4-2. Corresponding requirements can be found in [SP-SEC-CompSpec-5.7 - Logging and Diagnostic](#)

## 6.4 DoS Resilience and Minimising Negative Impact

 , **SP-SEC-Comm-6.4-1** - DoS resilience for communication interfaces is required by EU CRA and IEC 62443-4-2.

Corresponding requirements can be found in [SP-SEC-CompSpec-5.4.4 Denial of service resilience](#)

 , **SP-SEC-Comm-6.4-2** - Minimising negative impact to network and to connected devices is required by EU CRA.

Corresponding requirements can be found in [SP-SEC-CompSpec-5.4.2 Host-based firewall](#)