Disclaimer

This document is

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

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

drafted by and belongs to EU Rail.

Maintenance

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

cybersecurity.review@ertms.be

Work Item Type	Icon	Rationale
System Requirement		Used for mandatory requirements.
Text		Used for prose text, e.g. as an introduction or for additional information. The contents of these work items are **not requirements.**
Definition		Used for term defintions. The contents of these work items are **not requirements.**

First draft version (01/2024) includes:

- internal review based on
  - UNISIG Subset 146
  - EULYNX BL4 R2 Eu.Doc.114, Eu.Doc.115
  - EUG 23E057-1A Security Measures

Second draft version (02/2024) includes

- updated according to review comments from 1st draft review
- OCSP removed
- OPC-UA Details added

Final draft version (03/2024) includes

- HTTP Communication

- OPC-UA Permissions

, **SP-SEC-COMMComm-32.1-1 -** This specification is a Functional Interface Specification (FIS) for the security layer of CCS components Secure Components required for interoperability in the European rail automation domain. **[**SPPRAMSS-3780 **]**

, **SP-SEC-COMMComm-32.2-1 -** This specification uses identifiers starting with "SP-SEC-Comm".

, **SP-SEC-Comm-2.2-** If another protocol is used for communication, the requirement of Chapter 6.6 of the Secure Component Specification is applicable. **[**SPPRAMSS-7360 **]**

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

, **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

SPPRAMSS-1698 - [RFC - 8446]
The Transport Layer Security (TLS) Protocol Version 1.3.

- TLS

Transport Layer Security

(source: ~~SPPRAMSS-1705~~ - [UNISIG Subset-146]) **[**SPPRAMSS-1699 **]**

- Authentication

The process to verify the identity of communicating peers.

(source: ~~SPPRAMSS-1705~~ - [UNISIG Subset-146]) **[**SPPRAMSS-1703 **]**

- Confidentiality

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

(source: ISO 27000-2018) **[**SPPRAMSS-1704 **]**

[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

- TLS endpoint

The TLS endpoint is a Secure Component using TLS-protected communication (client and server). **[**SPPRAMSS-7301 **]**

- 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).

First release (V1.0) - February 2025

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

, SP-SEC-COMMComm-43-1 - Note: This chapter applies to all communication that uses TLS. **[**SPPRAMSS-7358 **]**

, **SP-SEC-COMMComm-43-2 -** 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. It is assumed that all migration topics are managed in the transition from an older baseline and release of the Technical Specification for Interoperability (TSI-CCS) to a newer one. **[**SPPRAMSS-2419 **]**

SP-SEC-Comm-3.1-1, , SP-SEC-COMM-4.1-1 - The TLS endpoint shall use TLS version 1.3 as defined in SP-SEC-Comm-2.3-4 - [RFC 8446]. **[**SPPRAMSS-1713 **]**

SP-SEC-Comm-3.1-2, , SP-SEC-COMM-4.1-2 - The TLS endpoint shall not use the zero round0-trip time RTT mode. **[**SPPRAMSS-1716 **]**

SP-SEC-Comm-3.1-3, , SP-SEC-COMM-4.1-3 - The TLS endpoint shall enforce mutual authentication. **[**SPPRAMSS-1954 **]**

SP-SEC-Comm-3.1-4, , SP-SEC-COMM-4.1-4 - The TLS endpoint shall use a cryptographically secure pseudorandom number generator (CSPRNG). **[**SPPRAMSS-3036 **]**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, , SP-SEC-COMM-4.1-5 - The TLS endpoint shall support the cipher TLS_AES_256_GCM_SHA384.
Note: This cipher is preferred.

SP-SEC-Comm-3.1-6, , SP-SEC-COMM-4.1-56 - If confidentiality protection is required, the The TLS endpoint shall support the cipher

TLS_CHACHA20_POLY1305_SHA256. **[**SPPRAMSS-1960 **]**

Note: This cipher is lower prioritized.

, **SP-SEC-COMM-4.1-6 -** If confidentiality protection is required, the TLS endpoint shall support the cipher TLS_AES_256_GCM_SHA384.
Note: Preferred cipher **[**SPPRAMSS-1959 **]**

SP-SEC-Comm-3.1-7, , SP-SEC-COMM-4.1-7 - If confidentiality only integrity protection is **not** required, the TLS endpoint shall use support the cipher

TLS_SHA384_SHA384. SPPRAMSSSP-2034 - SEC-Comm-2.3-5 - [RFC 9150] **[**SPPRAMSS-1961 **]**

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-COMMComm-43.1-8 -** Note: In future version of this document, the ciphers for securing communication awill will be extended to support additional ciphersciphers, e.g. for post quantum cryptography (PQC). **[**SPPRAMSS-10108 **]**

SP-SEC-Comm-3.2-1, , SP-SEC-COMM-4.2-1 - The TLS endpoint shall perform authentication using certificates in accordance with SPPRAMSS-6723. **[**SPPRAMSS-2030 **]**SP-SEC-Serv-6.3-2.

SP-SEC-Comm-3.2-2, , SP-SEC-COMM-4.2-2 - The TLS endpoint shall send the full certificate chain when initiating a TLS handshake. **[**SPPRAMSS-9980 **]**

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, , SP-SEC-COMM-4.2-3 - 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, , SP-SEC-COMM-4.2-4 - 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, , SP-SEC-COMM-4.2-5 - 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, , SP-SEC-COMM-4.2-6 - 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, , SP-SEC-COMM-4.2-37 - 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.).

NOTENote: This includes checking the certificate revocation status using CRLs of all certificates in the certificate path (excluding self-signed trust anchors). **[**SPPRAMSS-2426 **]**

SP-SEC-Comm-3.2-8, , SP-SEC-COMM-4.2-48 - If the status of a certificate is revoked or no valid certificate revocation information is available, the TLS endpoint shall abort the connection setup. **[**SPPRAMSS-2427 **]**

SP-SEC-Comm-3.2-9, , SP-SEC-COMM-4.2-59 - The TLS endpoint shall re-validate the communication partners partner's certificate including the revocation status at least every 24 hours. **[**SPPRAMSS-5999 **]**

SP-SEC-Comm-3.2-10, , SP-SEC-COMM-4.2-610 - If the re-validation of a certificate fails, the TLS endpoint shall terminate the TLS connection and re-establish a new TLS connection. **[**SPPRAMSS-6000 **]**

SP-SEC-Comm-3.2-11, , SP-SEC-COMM-4.2-711 - If the TLS communication is not safety-related, the TLS endpoint shall use an ONCC as defined in SPPRAMSS-7649. **[**SPPRAMSS-8869 **]**SP-SEC-Serv-14.1.2-2

SP-SEC-Comm-3.2-12, , SP-SEC-COMM-4.2-812 - If the TLS communication is safety-related, the TLS endpoint shall use an OSCC as defined in SPPRAMSS-7650. **[**SPPRAMSS-8870 **]**SP-SEC-Serv-14.1.2-3

SP-SEC-Comm-3.3-1, , SP-SEC-COMM-4.3-1 - The TLS endpoint shall log all the events caused by alert messages defined in SPPRAMSS-1698 - 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] Appendix B, Chapter 6.2. "Alert Messages" using SSI-LOG.
[SPPRAMSS-5857 **]**

, **SP-SEC-COMMComm-54-1 -** Note: This chapter applies to all communication that uses OPC UA. **[**SPPRAMSS-7357 **]**

, **SP-SEC-COMM-5-2 -** The OPC UA endpoint shall implement ~~SPPRAMSS-2956~~ - [ISO 62541-x:2020] . **[**SPPRAMSS-2954 **]**

SP-SEC-Comm-4-2, , **SP-SEC-COMM-5-32 -** The OPC UA endpoint shall use Secure Conversation (UASC) (SPPRAMSSSP-2957 - SEC-Comm-2.3-6 - [OPC UA-10000-6] , chapter Chapter 6.7) **[**SPPRAMSS-2952 **]**

SP-SEC-Comm-4-3, , **SP-SEC-COMM-5-43 -** The OPC UA endpoint shall use SignAndEncrypt as security mode. **[**SPPRAMSS-2953 **]**

SP-SEC-Comm-4-4, , **SP-SEC-COMM-5-54 -** The OPC UA endpoint shall use mutual authentication via certificates. **[**SPPRAMSS-2951 **]**

SP-SEC-Comm-4-5, , **SP-SEC-COMM-5-65 -** The OPC UA endpoint shall enforce the permissions attached to each node of the OPC-UA model. **[**SPPRAMSS-4951 **]**

SP-SEC-Comm-4-6, , **SP-SEC-COMM-5-76 -** If the The OPC UA endpoint supports the Profile Group UACore 1.05 or higher, the OPC UA endpoint shall support the Security Policy [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. **[**SPPRAMSS-7325 **]**]

SP-SEC-Comm-4-7, , **SP-SEC-COMM-5-87 -** If the The OPC UA endpoint supports the Profile Group UACore 1.05 or higher, the OPC UA endpoint shall support the Security Policy ECC-brainpoolP256r1. **[** SPPRAMSS-7352 **]**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-COMMComm-54-98 -** The OPC UA endpoint shall may support the Security Policy [Policy SP-SEC-Comm-2.3-9 - [OPC UA Profile SecurityPolicy [B] – Basic256Sha256.]

NOTENote: The preferred Security Policies are the ones using Elliptic Curve Cryptography (ECC). Support for RSA is may be required for backwards compatibility to Profile Group UACore 1.04 or lower that implementations which do not support ECC yet. RSA will be removed in a future version of this specification. **[**SPPRAMSS-7328 **]**

SP-SEC-Comm-4-9, , **SP-SEC-COMM-5-109 -** The OPC UA endpoint shall support the following permissions: **[**SPPRAMSS-8867 **]**

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`

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

`eu.era.sdi.diagnostic-read`	Permission to read OPC UA nodes containing diagnostic information (e.g. hardware or operating system diagnostics).	`Browse`
		`Read`
		`ReceiveEvents`

`eu.era.smi.software-distribute`	Permission to distribute software update/configuration/engineering data to devices.	`Browse`
		`Read`
		`Execute`
		`ReceiveEvents`

`eu.era.smi.software-activate`	Permission to execute OPC UA methods to activate previously distributed software update/configuration/engineering data update.	`Browse`
		`Read`
		`Execute`
		`ReceiveEvents`

`eu.era.ssi.security-read`	Permission to read OPC UA nodes containing security-related information.	`Browse`
		`Read`
		`ReceiveEvents`

`eu.era.ssi.security-execute`	Permission to execute OPC UA methods to execute security-related methods.	`Browse` `Execute`
`eu.era.smi.component-reset`	Permission to reset component. This is a seperate permission since it has impact on availability.	`Browse` `Execute`

, SP-SEC-COMMComm-54-1110 - 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-COMMComm-54-1211 -** The permissions are retrieved via the SSI-IAM interface and enforced by the Secure Component. (see SPPRAMSS-2311) **[**SPPRAMSS-9756 **]**SP-SEC-Comp-7.2-2)

, **SP-SEC-COMM-6-1 -** The HTTP endpoint shall use HTTP/2 as defined in RFC 9113. **[**SPPRAMSS-8865 **]**

SP-SEC-Comm-5-1, , **SP-SEC-COMM-6-21 -** The HTTP endpoint shall use TLS for HTTP communication according to 43 - End-to-End Security Layer (TLS). **[**SPPRAMSS-8864 **]**

, **SP-SEC-COMMComm-65-32 -** Exceptions for the usage of TLS for HTTP communication are defined in the Shared Cybersecurity Services Specification. **[**SPPRAMSS-10322 **]**

, **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)

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.

SP-SEC-Comm-6.1-1, , **SP-SEC-COMM-7.1-1 -** 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, diagnositc server,...), not per software process instance of the same software process.

SP-SEC-Comm-6.1-2, , **SP-SEC-COMM-7.1-2 -** 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, , **SP-SEC-COMM-7.1-3 -** 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, , SP-SEC-COMM-7.1-4 - 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.

SP-SEC-Comm-6.2-1, , SP-SEC-COMM-7.2-1 - 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, , SP-SEC-COMM-7.2-2 - 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.

, 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

, 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