



**EULYNX Initiative**

## **EULYNX Security Parameter Specification**

Document number: Eu.Doc.115  
Version: 1.1 (0.A)

Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Release information	1
1.2	Impressum	1
1.3	Purpose	1
1.4	Applicable standards and regulations	2
1.5	Applicable documents	2
1.6	Terms and abbreviations	2
1.7	Variability management	2
1.8	Definition of object types	2
<b>2</b>	<b>Requirements for the network</b>	<b>2</b>
2.1	OSI layer 4: Port	2
<b>3</b>	<b>Requirements for TLS implementation</b>	<b>3</b>
3.1	Endpoints	3
3.2	Certificate	3
3.3	TLS version	3
3.4	Handshake	3
3.5	Key exchange / key agreement	3
3.6	Digital signature	3
3.7	Ciphers	3
<b>4</b>	<b>Requirements for IPsec used within Variant A (Crypto Box)</b>	<b>4</b>
4.1	Certificate	4
4.2	Ciphers	4
4.3	Key exchange	4
<b>5</b>	<b>Requirements for Hash Algorithms</b>	<b>4</b>
<b>6</b>	<b>Requirements for Encryption of Data at Rest</b>	<b>4</b>
<b>7</b>	<b>Requirements for Time services</b>	<b>4</b>
<b>8</b>	<b>Requirements for OPC-UA</b>	<b>5</b>
<b>9</b>	<b>Requirements for Recovery keys</b>	<b>5</b>
<b>10</b>	<b>Requirements for SNMP</b>	<b>5</b>
<b>11</b>	<b>Outdated protocols which shall not be used</b>	<b>5</b>

ID	Type	Requirement	Valid for
Eu.Sec-Par.1	Head	<b>1 Introduction</b>	
Eu.Sec-Par.2	Head	<b>1.1 Release information</b>	
Eu.Sec-Par.3	Info	[Eu.Doc.115] EULYNX Security Parameter Specification CENELEC Phase: 4 Version: 1.1 (0.A) Approval date: 15.06.2023	--
Eu.Sec-Par.4	Info	<b>Version history</b>	--
Eu.Sec-Par.5	Info	version number: 0.1 (0.A) date: 22.12.2021 author: Robert Hughes, Ulrich Meier, Richard Poschinger, André Rumbold, Geir Rydland, Jaco Schoonen, Max Schubert, David Shipman review: security cluster changes: initial version in Doors	--
Eu.Sec-Par.159	Info	version number: 1.0 (0.A) date: 17.05.2022 author: Robert Hughes, Ulrich Meier, Richard Poschinger, André Rumbold, Geir Rydland, Jaco Schoonen, Max Schubert, David Shipman review: CCB changes: editorial corrections and changes from CCB and UNIFE review	--
Eu.Sec-Par.167	Info	version number: 1.1 (0.A) date: 28.06.2023 author: Ulrich Meier, Richard Poschinger, Nicolas Poyet, Max Schubert review: Security cluster + CCB changes: Full rework for Baseline 4 Release 2	--
Eu.Sec-Par.6	Head	<b>1.2 Impressum</b>	
Eu.Sec-Par.7	Info	Publisher: <b>EULYNX Initiative</b>  A full list of the <b>EULYNX Partners</b> can be found on <a href="http://www.eulynx.eu/index.php/members">www.eulynx.eu/index.php/members</a>	--
Eu.Sec-Par.8	Info	Responsible for this document: EULYNX Project Management Office <a href="http://www.eulynx.eu">www.eulynx.eu</a>	--
Eu.Sec-Par.9	Info	Copyright EULYNX Partners All information included or disclosed in this document is licensed under the European Union Public Licence EUPL, Version 1.2 or later.	--
Eu.Sec-Par.10	Head	<b>1.3 Purpose</b>	
Eu.Sec-Par.11	Info	The purpose of this document is to define the security requirements for the parameters referenced in the EULYNX Security Specifications [EU.Doc.114] which are expected to be changed frequently. These requirements are specified for the whole EULYNX architecture, including communication interfaces and system components.	--
Eu.Sec-Par.12	Info	Additional protocols beyond EULYNX interfaces or named in this document should be avoided.	--
Eu.Sec-Par.13	Info	The protocols should be used as specified to ensure interoperability.	--
Eu.Sec-Par.14	Info	The concept for security is documented in the EULYNX Security Concept [Eu.Doc.15]. The detailed specifications for security are documented in the EULYNX Security Specifications [Eu.Doc.114].	--
Eu.Sec-Par.15	Info	Inputs for the document are the systems operational environment, applicable security standards as well as purpose and scope of the system.	--
Eu.Sec-Par.16	Info	Having a security concept at EULYNX level will facilitate alignment with other infrastructure managers and European bodies, because the same language and terminology is used.	--
Eu.Sec-Par.17	Info	All requirements are based on the EULYNX risk assessment. If the IM is not following these recommendations, the IM must ensure that his security level is maintained.	--

ID	Type	Requirement	Valid for
Eu.Sec-Par.157	Info	This document is intended for the following users: <ul style="list-style-type: none"> <li>• safety authorities</li> <li>• infrastructure managers</li> <li>• safety assessors</li> <li>• signalling system suppliers</li> <li>• validators</li> <li>• security assessors</li> </ul>	--
Eu.Sec-Par.158	Info	The applicability of each requirement either exclusively for the infrastructure manager or for all relevant parties is indicated by the column "Valid for".  Note: 'All parties' may include suppliers of signalling system components and suppliers of other components dedicated to IT security.	--
Eu.Sec-Par.165	Info	The following statements should be considered before applying the specification: <ul style="list-style-type: none"> <li>• The security documents of the following enumeration shall be referred and used only as a complete set. <ul style="list-style-type: none"> <li>o Eu.Doc.15</li> <li>o Eu.Doc.114</li> <li>o Eu.Doc.115</li> <li>o Eu.Doc.116</li> <li>o Eu.Doc.117</li> <li>o Eu.Doc.121</li> </ul> </li> <li>• Development of the specification is based on IEC 62443 process, together with TS 50701 railway specification application suggestions.</li> <li>• If the infrastructure manager (IM) applies the Security Specification, the IM must be aware that successful implementation requires a detailed analysis and adoption of, at least, the IM's rollout and maintenance procedures.</li> <li>• The specifications contains options that need to be decided carefully by the IM due to impact to feasibility in migration, business activity, process adoption for operation (rollout, maintenance,...), tender process, possible suppliers, and costs (CAPEX, OPEX).</li> <li>• The current specification does not contain testing requirements for the suppliers. So, the test type (testing, audit, analysis, demonstration) and its acceptance criteria should be defined before using the documents in tender process.</li> </ul>	--
Eu.Sec-Par.19	Head	<b>1.4 Applicable standards and regulations</b>	
Eu.Sec-Par.18	Info	A list of applicable standards and regulations used in EULYNX is listed in the EULYNX Reference Document List [Eu.Doc.12].	--
Eu.Sec-Par.20	Info	This document refers to technical standards which are mentioned in the requirement chapters.	--
Eu.Sec-Par.21	Head	<b>1.5 Applicable documents</b>	
Eu.Sec-Par.22	Info	The current versions of EULYNX documents used as input or related to this document are listed in the EULYNX Documentation Plan [Eu.Doc.11]. The relationships between the documents are displayed in the Appendix A1 Documentation plan and structure [Eu.Doc.11_A1].	--
Eu.Sec-Par.23	Head	<b>1.6 Terms and abbreviations</b>	
Eu.Sec-Par.24	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9].	--
Eu.Sec-Par.25	Head	<b>1.7 Variability management</b>	
Eu.Sec-Par.26	Info	This document is valid for the complete EULYNX System. Variability management is not used in this document.	--
Eu.Sec-Par.27	Head	<b>1.8 Definition of object types</b>	
Eu.Sec-Par.28	Info	The following definition for object types is applied in this document:	--
Eu.Sec-Par.29	Info	• "Req" - This denotes a mandatory requirement.	--
Eu.Sec-Par.30	Info	• "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.	--
Eu.Sec-Par.31	Info	• "Head" - This denotes chapter headings.	--
Eu.Sec-Par.32	Head	<b>2 Requirements for the network</b>	
Eu.Sec-Par.33	Head	<b>2.1 OSI layer 4: Port</b>	

ID	Type	Requirement	Valid for
Eu.Sec-Par.34	Req	The component shall provide the user with the ability to configure the ports.	All
Eu.Sec-Par.38	Head	<b>3 Requirements for TLS implementation</b>	
Eu.Sec-Par.39	Info	TLS requirements are set very narrow to ensure interoperability and timing.	--
Eu.Sec-Par.42	Head	<b>3.1 Endpoints</b>	
Eu.Sec-Par.43	Info	The entities that shall use TLS endpoints are defined in Eu.Doc.114.	--
Eu.Sec-Par.46	Head	<b>3.2 Certificate</b>	
Eu.Sec-Par.47	Req	The TLS certificate shall use X.509v3.	All
Eu.Sec-Par.168	Req	The TLS certificate shall use 256 bit ECDSA signatures.	All
Eu.Sec-Par.50	Req	The IM shall include requirements regarding updateability of the certificate signature according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.51	Head	<b>3.3 TLS version</b>	
Eu.Sec-Par.52	Req	The TLS endpoint shall use TLS 1.3.	All
Eu.Sec-Par.54	Req	The IM shall include requirements regarding updateability of the TLS version according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.55	Head	<b>3.4 Handshake</b>	
Eu.Sec-Par.56	Req	The TLS endpoint shall use the handshake methodology 1-RTT.	All
Eu.Sec-Par.57	Head	<b>3.5 Key exchange / key agreement</b>	
Eu.Sec-Par.58	Req	The TLS endpoint shall provide the key exchange method x25519.	All
Eu.Sec-Par.169	Req	The TLS endpoint shall provide the key exchange method secp256r1.	All
Eu.Sec-Par.170	Req	The TLS endpoint shall use the key exchange method x25519 by default.	All
Eu.Sec-Par.60	Req	The IM shall include requirements regarding updateability of the key exchange/agreement method according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.61	Head	<b>3.6 Digital signature</b>	
Eu.Sec-Par.62	Req	The TLS endpoint shall provide the digital signature algorithm Ed25519.	All
Eu.Sec-Par.171	Req	The TLS endpoint shall provide the digital signature algorithm ecdsa_secp256r1_sha256.	All
Eu.Sec-Par.172	Req	The TLS endpoint shall use the digital signature algorithm Ed25519 by default	All
Eu.Sec-Par.64	Req	The IM shall include requirements regarding updateability for digital signature according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.65	Head	<b>3.7 Ciphers</b>	
Eu.Sec-Par.66	Req	The TLS endpoint shall provide the cipher TLS_AES_256_GCM_SHA384.	All
Eu.Sec-Par.173	Req	The TLS endpoint shall provide the cipher TLS_CHACHA20_POLY1305_SHA256.	All
Eu.Sec-Par.174	Req	The TLS endpoint shall provide the cipher TLS_AES_128_GCM_SHA256.	All
Eu.Sec-Par.67	Req	The TLS endpoint shall provide the cipher TLS_SHA384_SHA384.	All
Eu.Sec-Par.69	Req	The list of activated cipher suites must be adjustable by the IM (e.g., deactivate integrity-only ciphers if encryption should be used for every connection or deactivate outdated cipher suites).	All

ID	Type	Requirement	Valid for
Eu.Sec-Par.70	Req	The entities shall provide the capability to permanently store the configuration which cipher is used in TLS-based communication. Note: This allows the IM to turn-off integrity based ciphers in a permanent way to prevent misconfigurations.	All
Eu.Sec-Par.73	Req	The IM shall include requirements regarding updateability for ciphers according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.74	Head	<b>4 Requirements for IPsec used within Variant A (Crypto Box)</b>	
Eu.Sec-Par.164	Info	Variant A is defined in the EULYNX Security Concept [Eu.Doc.15].	--
Eu.Sec-Par.75	Info	As the implementation of Variant A (Crypto Box) is defined outside EULYNX, the IM must ensure that the required security level is reached for the application. For EULYNX purposes this security level is set to be at least 3.	--
Eu.Sec-Par.76	Info	As Variant A is proprietary and in the EULYNX architecture part of the subsystem communication-system without interoperability requirements, it is up to the IM to ensure interoperability between different implementations.	--
Eu.Sec-Par.77	Head	<b>4.1 Certificate</b>	
Eu.Sec-Par.78	Req	The Variant A endpoint shall use certificates with an equal or stronger signature algorithm as defined in the requirements for TLS.	All
Eu.Sec-Par.81	Head	<b>4.2 Ciphers</b>	
Eu.Sec-Par.82	Req	The Variant A endpoint shall use equal or stronger ciphers as defined in the requirements for TLS.	All
Eu.Sec-Par.83	Head	<b>4.3 Key exchange</b>	
Eu.Sec-Par.84	Req	The Variant A endpoint shall use equal or stronger key exchange method as defined in the requirements for TLS.	All
Eu.Sec-Par.85	Head	<b>5 Requirements for Hash Algorithms</b>	
Eu.Sec-Par.86	Info	Hash functionality or hash values on their own do not protect integrity.	--
Eu.Sec-Par.87	Req	If the integrity protection of Variant A, B and C cannot be used for protecting data in transit then the endpoint shall provide the hash algorithm SHA256.	All
Eu.Sec-Par.175	Req	If the integrity protection of Variant A, B and C cannot be used for protecting data in transit then the endpoint shall provide the hash algorithm Curve25519.	All
Eu.Sec-Par.176	Req	If the integrity protection of Variant A, B and C cannot be used for protecting data in transit then the endpoint shall provide the IM with the ability to configure the hash algorithm.	All
Eu.Sec-Par.177	Req	If the integrity protection of Variant A, B and C cannot be used for protecting data in transit then the endpoint shall use the hash algorithm selected by the IM.	All
Eu.Sec-Par.88	Req	If data at rest must be protected then the component shall provide the hash algorithm SHA512.	All
Eu.Sec-Par.178	Req	If data at rest must be protected then the component shall provide the hash algorithm Curve25519.	All
Eu.Sec-Par.90	Req	If data at rest must be protected then the component shall provide the IM with the ability to configure the hash algorithm.	All
Eu.Sec-Par.179	Req	If data at rest must be protected then the component shall use the hash algorithm selected by the IM.	All
Eu.Sec-Par.91	Req	The IM shall include requirements regarding updateability for hash algorithms according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.92	Head	<b>6 Requirements for Encryption of Data at Rest</b>	
Eu.Sec-Par.93	Req	If data at rest must be encrypted, the component shall use AES 256 for encryption	All
Eu.Sec-Par.96	Req	The IM shall include requirements regarding updateability for encryption algorithms according to upcoming releases of Eu.Doc.115 in its tender.	IM
Eu.Sec-Par.97	Head	<b>7 Requirements for Time services</b>	
Eu.Sec-Par.98	Req	The component shall use time synchronisation protocol NTPv4.	All
Eu.Sec-Par.101	Req	While operation, the component shall ensure a maximum time deviation to the time base of 1 minute	All

ID	Type	Requirement	Valid for
Eu.Sec-Par.102	Req	If time stamp authority is used, the time server shall received it's time from an ASC X9.95 certified time source authority (TSA).	All
Eu.Sec-Par.103	Req	The IM shall decide, if access to a time stamp authority (TSA) is required	IM
Eu.Sec-Par.104	Head	<b>8 Requirements for OPC-UA</b>	
Eu.Sec-Par.105	Info	Within EULYNX OPC UA is to be used for SMI and SDI applications as defined in the Interface definition and specification SMI [Eu.Doc.76] and the Interface definition SDI [Eu.Doc.77].	--
Eu.Sec-Par.106	Req	The OPC-UA endpoint shall implement ISO 62541-x:2020.	All
Eu.Sec-Par.107	Req	The OPC-UA endpoint shall use Secure Conversation (UASC) (ref OPC UA-10000-6, chapter 6.7)	All
Eu.Sec-Par.108	Req	The OPC-UA endpoint shall use SignAndEncrypt as security mode.	All
Eu.Sec-Par.109	Req	The OPC-UA endpoint shall use a secure channel using Basic256SHA256 (binary UASC).	All
Eu.Sec-Par.111	Req	The OPC-UA endpoint shall use mutual authentication via certificates.	All
Eu.Sec-Par.118	Head	<b>9 Requirements for Recovery keys</b>	
Eu.Sec-Par.119	Req	If the usage of recovery keys is permitted by the IM and used to protect data for over one week, the component shall use recovery keys with a minimum length of 100 bits.	All
Eu.Sec-Par.120	Req	If the usage of recovery keys is permitted by the IM and used to protect data for less than one week, the component shall use recovery keys with a minimum length of 32 bits.	All
Eu.Sec-Par.131	Head	<b>10 Requirements for SNMP</b>	
Eu.Sec-Par.132	Info	For SMI and SDI applications, OPC-UA is the specified solution within EULYNX starting with baseline 3.	--
Eu.Sec-Par.133	Info	If SNMP is used either for a) non-compliant EULYNX devices not capable of OPC UA/SDI or b) non-EULYNX devices communicating with MDM or other EULYNX sub-system the following requirements apply:	--
Eu.Sec-Par.134	Req	If SNMP is used for communication between the endpoint and MDM, the SNMP endpoint shall use SNMP v3.	All
Eu.Sec-Par.135	Req	If SNMP is used for communication between the endpoint and MDM, the SNMP endpoint shall use AuthPriv for Authentication and Encryption.	All
Eu.Sec-Par.136	Info	SNMP v3 can use User-base Security Model, USM, RFC 3414; or Transport-based Security Model, TSM, RFC 5591. It is recommended to use Transport-based Security Model as it can be integrated into the security systems already available for security TLS for SCI.	--
Eu.Sec-Par.137	Req	The SNMP endpoint shall be configured by the IM using the least privilege principle.	IM
Eu.Sec-Par.150	Head	<b>11 Outdated protocols which shall not be used</b>	
Eu.Sec-Par.151	Req	The EULYNX system shall not use TELNET.	All
Eu.Sec-Par.181	Req	The EULYNX system shall not use TLS 1.0.	All
Eu.Sec-Par.182	Req	The EULYNX system shall not use TLS 1.1.	All
Eu.Sec-Par.152	Info	Other old or outdated protocols not mentioned but widely known to be unsecure or imposing a security risk avoidable, should not be used.	--
Eu.Sec-Par.153	Req	If the IM must use outdated protocols in the EULYNX system, the IM shall assess the risk before approving the use.	IM