



EULYNX Initiative

Interface definition and specification SSI

Document number: Eu.Doc.117
Version: 1.1 (0.A)

Contents

1	Introduction	1
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
2	Requirements	2
2.1	Definition of the SSI	2
2.1.1	Physical interface	2
3	SSI-XX-PKI: Public Key Infrastructure	2
4	SSI-XX-SLOG: Security Logging	3
4.1	Overall logging service requirements and definitions:	3
4.2	Generic Log Message	4
4.3	Generic requirements for logging protocols	5
4.3.1	Syslog	5
4.3.2	OPC UA	5
4.4	Log Requirements	5
4.4.1	Log Requirements for Logging Services	5
4.4.1.1	Interrupted Logging Connection Detected: sec.log.interr	5
4.4.1.2	Outdated Logging Data Detected: sec.log.outd	5
4.4.1.3	Corruption of Logging Data Detected: sec.log.corr	6
4.4.1.4	Missing Logging Data Detected: sec.log.misrcv	6
4.4.1.5	Timestamp Mismatch: sec.log.tmis	6
4.4.1.6	Timestamp Inconsistency Detected: sec.log.tsinc	6
4.4.1.7	Data Already Received: sec.log.drcv	6
4.4.1.8	Missing Log Data Detected in Storage: sec.log.misys	6
4.4.1.9	Logging Capacity Storage Reached: sec.log.capw	6
4.4.1.10	Logging Capacity Storage Reached Alert: sec.log.capa	7
4.4.2	Log requirements for Networked Devices	7
4.4.2.1	Packet Drop: sec.net.dev.dp	7
4.4.2.2	Network Interface Card Down: sec.net.dev.ndw	7
4.4.2.3	Network Interface Card Up: sec.net.dev.nup	7
4.4.2.4	TCP Reset Segment Received: sec.net.dev.tcprst	7

4.4.2.5	Martian Packet Received: sec.net.dev.mp	7
4.4.2.6	New DHCP Lease Requested: sec.net.dev.ndreq	7
4.4.2.7	DHCP New IP Received: sec.net.dev.ndesp	8
4.4.2.8	Firewall Warnings and Blocked Connections: sec.net.dev.fwbc	8
4.4.2.9	Firewall Warning: sec.net.dev.fww	8
4.4.2.10	Change in Cabling Detected: sec.net.dev.chcbl	8
4.4.2.11	Detect Physical Port Speed Change: sec.net.dev.chspd	8
4.4.2.12	Connection Attempt to Management Port: sec.net.dev.camp	8
4.4.2.13	Too Many Open Sockets: sec.net.dev.tmc	8
4.4.2.14	Disabled TCP or UDP Port Activated: sec.net.dev.dlprta	8
4.4.2.15	Internal Errors: sec.net.dev.ierr	9
4.4.2.16	Internal Warning: sec.net.dev.iwarn	9
4.4.2.17	Shutdown due to Security Error: sec.net.dev.isec	9
4.4.2.18	Packet Blocked: sec.net.dev.caprt	9
4.4.2.19	Authentication failed: sec.net.dev.caauth	9
4.4.3	Log requirements for Network Security Components	9
4.4.3.1	Network Security Component Warning: sec.net.sec.warn	9
4.4.3.2	Firewall Blocked Connection: sec.net.sec.blc	10
4.4.3.3	Denial of Service Detected: sec.net.sec.dos	10
4.4.3.4	Malicious Content: sec.net.sec.mc	10
4.4.4	Log requirements for RaSTA	10
4.4.4.1	RaSTA Connection Terminated due to Sequence Error: sec.rasta.tdse	10
4.4.4.2	RaSTA Payload: sec.rasta.pct	10
4.4.4.3	RaSTA Connection Failed: sec.rasta.fce	10
4.4.4.4	RaSTA Redundancy Channel Connection Established: sec.rasta.rcest	11
4.4.4.5	RaSTA Safety Channel Connection Established: sec.rasta.sacest	11
4.4.4.6	RaSTA Channel A Connection Established: sec.rasta.cra	11
4.4.4.7	RaSTA Channel B Connection Established: sec.rasta.crb	11
4.4.4.8	RaSTA Channel C Connection Established: sec.rasta.crc	11
4.4.4.9	RaSTA Redundancy Channel Connection Lost: sec.rasta.lrc	11
4.4.4.10	RaSTA Redundancy Channel A Lost: sec.rasta.lrca	11
4.4.4.11	RaSTA Redundancy Channel B Lost: sec.rasta.lrcb	11
4.4.4.12	RaSTA Redundancy Channel C Lost: sec.log.lrcc	12
4.4.4.13	RaSTA Heartbeat Missing: sec.rasta.hbm	12
4.4.4.14	RaSTA Resend Triggered: sec.rasta.rst	12
4.4.4.15	RaSTA Connection Request: sec.rasta.crd	12
4.4.4.16	RaSTA Termination Request: sec.rasta.rctr	12
4.4.4.17	RaSTA Connection Terminated: sec.rasta.rct	12
4.4.4.18	RaSTA Redundancy Layer Error: sec.rasta.emr	13
4.4.4.19	RaSTA Safety Layer Error: sec.rasta.ems	13
4.4.4.20	RaSTA Transport Layer Error: sec.rasta.emta	13
4.4.5	Log requirements for OPC UA	13

4.4.5.1	Binary Secure Conversation Requested: sec.opcua.bscr	13
4.4.5.2	Binary Secure Conversation Established: sec.opcua.bsce	14
4.4.5.3	Binary Secure Conversation Connection Establishment Failed: sec.opcua.bscf	14
4.4.5.4	Binary Secure Conversation Connection Error: sec.opcua.embsc	14
4.4.6	Log requirements for Network Access Control	14
4.4.6.1	NAC Disconnect or Connect: sec.net.nac.popi	14
4.4.6.2	NAC Invalid Certificate: sec.net.nac.cic	14
4.4.6.3	Network Access Granted: sec.net.nac.cvc	14
4.4.6.4	NAC Network Access Timeout: sec.net.nac.rvk	14
4.4.7	Log requirements for TLS	15
4.4.7.1	TLS Dropped Connection - Sequence Error: sec.tls.dcse	15
4.4.7.2	TLS Connection Attempt with Invalid Certificate: sec.tls.cic	15
4.4.7.3	TLS Invalid Certificate: Rid field invalid: sec.tls.cicrid	15
4.4.7.4	TLS Connection Attempt with Invalid Certificate (Root not trusted): sec.tls.cicrc	15
4.4.7.5	TLS Connection Attempt with Invalid Certificate (Certificate Expired): sec.tls.cicte	15
4.4.7.6	TLS Connection Attempt with Certificate not Authorised for Connection: sec.tls.cicna	16
4.4.7.7	TLS Connection Established: sec.tls.cvc	16
4.4.7.8	Dropped TLS due to Transport Layer Error: sec.tls.dcte	16
4.4.7.9	TLS Failed to Establish Connection: sec.tls.cf	16
4.4.7.10	TLS Connection Attempt Failed due to Invalid Cipher: sec.tls.cfci	17
4.4.7.11	TLS Connected: sec.tls.cuci	17
4.4.7.12	TLS Connection Attempt Failed due to Wrong Key Exchange Method: sec.tls.cfwke	17
4.4.7.13	TLS Error of Underlying Library: sec.tls.emtls	17
4.4.7.14	TLS Connect Request: sec.tls.cr	17
4.4.7.15	TLS Terminate Request: sec.tls.ct	18
4.4.8	Log requirements for Interlocking (EIL) (sec.eil.*)	18
4.4.8.1	Misconfigured Connections Detected: sec.eil.miscon	18
4.4.8.2	Misconfigured Aystem Associations Detected: sec.eil.missys	18
4.4.8.3	EfeS Unavailable: sec.eil.ccuV	18
4.4.8.4	EfeS Connection Timeout: sec.eil.occt	18
4.4.8.5	RBC Connection Timeout: sec.eil.rbcct	18
4.4.8.6	TCS Connection Timeout: sec.eil.tbcct	18
4.4.8.7	Failure of EfeS Area Detected: sec.eil.fare	18
4.4.9	Log requirements for systems connected via SCI-XX.PDI (sec.pdi.*)	18
4.4.9.1	Misconfigured Connections Detected: sec.pdi.miscon	18
4.4.9.2	Misconfigured System Associations Detected: sec.pdi.missys	18
4.4.9.3	Connection Timeout: sec.pdi.timeout	19
4.4.9.4	Packet not Treated due to Failed Identifier Check: sec.pdi.idchk	19
4.4.9.5	PDI Connection Closed: sec.pdi.closed	19
4.4.10	Log Requirements for Components	19
4.4.10.1	Connection to Device Established: sec.efes.cest	19
4.4.10.2	Connection Attempt to Device Failed: sec.efes.cfai	19

4.4.10.3	Connection Attempt to Device Rejected: sec.efes.crej	19
4.4.10.4	Connection Attempt to Management Port: sec.efes.mgmt	19
4.4.10.5	Disabled Port Activated / In Use: sec.efes.dprta	19
4.4.10.6	Report on Activated Ports: sec.efes.rprt	19
4.4.10.7	Detected State Change Changing in Connections/Cabling: sec.efes.cbl	20
4.4.10.8	Installation/Deployment of Software/Configarutions Started/Finished: sec.efes.depl	20
4.4.10.9	Component Integrity Check Failed: sec.efes.intcf	20
4.4.10.10	Component Integrity Check Failed: sec.comp.intcf	20
4.4.10.11	Component Integrity Check Successful: sec.efes.intcs	20
4.4.10.12	Component Integrity Check Successful: sec.comp.intcs	20
4.4.10.13	Overheat Detected (in cabinet): sec.efes.heatc	20
4.4.10.14	Overheat Detected in Surrounding Environment: sec.comp.heatc	20
4.4.10.15	Overheat Detected in Device: sec.efes.heatd	20
4.4.10.16	Overheat Detected in Component: sec.comp.heatd	20
4.4.11	Log requirements for MDM	20
4.4.11.1	Deployment Started: sec.mdm.depl	20
4.4.11.2	Deployment Started: sec.mdm.deplb	20
4.4.11.3	Deployment Finished: sec.mdm.deple	21
4.4.11.4	Integrity Check of Component Failed: sec.mdm.intcf	21
4.4.11.5	Integrity Check of Component Successful: sec.mdm.intcs	21
4.4.11.6	Device not Available: sec.mdm.unav	21
4.4.11.7	Unkown Device: sec.mdm.devuk	21
4.4.11.8	Unknown Connection Identified: sec.mdm.conuk	21
4.4.12	Log requirements for Backup Services	21
4.4.12.1	Backup Started: sec.ssi.backup.started	21
4.4.12.2	Backup Received: sec.ssi.backup.rec	21
4.4.12.3	Backup Rejected due to Integrity Check Failure: sec.ssi.backup.rej	22
4.4.12.4	Backup Requested: sec.ssi.backup.req	22
4.4.12.5	Restore Started: sec.ssi.backup.reststarted	22
4.4.12.6	Restore Completed: sec.ssi.backup.restcomp	22
4.4.12.7	Backup Request Rejected: sec.ssi.backup.reqf	22
4.4.12.8	Backup Connection Rejected: sec.ssi.backup.crej	22
4.4.12.9	Backup Authorisation Failed: sec.ssi.backup.af	22
4.4.12.10	Missing Backup Detected: sec.ssi.backup.miss	22
4.4.12.11	Corrupted or Damaged Backup Detected: sec.ssi.backup.dmg	23
4.4.12.12	Error Saving Backup: sec.ssi.backup.svgerr	23
4.4.12.13	Error in Backup Connection: sec.ssi.backup.conerr	23
4.4.12.14	Connection Aborted by Client: sec.ssi.backup.conabo	23
4.4.12.15	Internal Error: sec.ssi.backup.interr	23
4.4.13	Log requirements for Time Services	23
4.4.13.1	Failed Time Synchronisation: sec.ssi.time.fts	23
4.4.13.2	Failed Time Synchronisation with Details: sec.ssi.time.ftsd	23

4.4.13.3	Time Synchronisation Successful: sec.ssi.time.sts	23
4.4.13.4	Time Synchronization Successful with Details: sec.ssi.time.stsd	23
4.4.14	Log requirements for Certificate Process	24
4.4.14.1	New Certificate Used: sec.ssi.cert.unc	24
4.4.14.2	New Certificate used by EIL: sec.ssi.cert.eil.unc	24
4.4.14.3	New Certificate used by EfeS: sec.ssi.cert.efes.unc	24
4.4.14.4	New Certificate used by MDM: sec.ssi.cert.mdm.unc	24
4.4.14.5	Renewal of Certificate: sec.ssi.cert.rnc	24
4.4.14.6	Renewal of Certificate for EIL: sec.ssi.cert.eil.rnc	24
4.4.14.7	Renewal of Certificate for EfeS: sec.ssi.cert.efes.rnc	24
4.4.14.8	Renewal of Certificate for MDM: sec.ssi.cert.mdm.rnc	24
4.4.14.9	Sending Signing Request for a Certificate: sec.ssi.cert.rec	24
4.4.14.10	Sending Signing Request of a Certificate for EIL: sec.ssi.cert.eil.rec	24
4.4.14.11	Sending Signing Request of a Certificate for EfeS: sec.ssi.cert.efes.rec	24
4.4.14.12	Sending Signing Request of a Certificate for MDM: sec.ssi.cert.mdm.rec	24
4.4.14.13	Update of CRL: sec.ssi.cert.ucrl	25
4.4.14.14	Update of CRL for EIL: sec.ssi.cert.eil.ucrl	25
4.4.14.15	Update of CRL for EfeS: sec.ssi.cert.eil.ucrl	25
4.4.14.16	Update of CRL for MDM: sec.ssi.cert.eil.ucrl	25
4.4.14.17	Issued New Certificate: sec.ssi.cert.inc	25
4.4.14.18	Receiving Signing Request for a Certificate: sec.ssi.cert.rnc	25
4.4.14.19	Receiving Signing Request for a Certificate by PKI RA: sec.ssi.cert.pki_ra.rnc	25
4.4.14.20	Receiving Signing Request for a Certificate by PKI CA: sec.ssi.cert.pki_ca.rnc	25
4.4.14.21	Revocation of Certificate: sec.ssi.cert.rec	25
4.4.14.22	Revocation of Certificate: sec.ssi.cert.pki_ca.rec	25
4.4.14.23	Failed Validation of Certificate: sec.ssi.cert.fvc	26
4.4.14.24	Failed Validation of Certificate for EIL: sec.ssi.cert.eil.fvc	26
4.4.14.25	Failed Validation of Certificate for EfeS: sec.ssi.cert.efes.fvc	26
4.4.14.26	Failed Validation of Certificate for MDM: sec.ssi.cert.mdm.fvc	26
4.4.14.27	Successful Validation of Certificate: sec.ssi.cert.pvc	26
4.4.14.28	Successful Validation of Certificate for EIL: sec.ssi.cert.eil.pvc	26
4.4.14.29	Successful Validation of Certificate for EfeS: sec.ssi.cert.efes.pvc	26
4.4.14.30	Successful Validation of Certificate for MDM: sec.ssi.cert.mdm.pvc	26
4.4.14.31	Failed Access to Validation Endpoint: sec.ssi.cert.facl	26
4.4.14.32	Failed Access to Validation Service for EIL: sec.ssi.cert.eil.facl	26
4.4.14.33	Failed Access to Validation Service for EfeS: sec.ssi.cert.efes.facl	26
4.4.14.34	Failed Access to Validation Service for MDM: sec.ssi.cert.mdm.facl	26
4.4.15	Log requirements for Identity and Access Management	27

ID	Type	Requirement
Eu.SSI.1	Head	1 Introduction
Eu.SSI.2	Head	1.1 Release information
Eu.SSI.3	Info	[Eu.Doc.117] Interface definition and specification SSI CENELEC Phase: 5 Version: 1.1 (0.A) Approval date: 15.06.2023
Eu.SSI.4	Info	Version history
Eu.SSI.5	Info	version number: 0.1 (0.A) date: 25.03.2022 author: Marius Rennmann, Max Schubert, Richard Poschinger, Ulrich Meier review: security cluster changes: initial version in Doors
Eu.SSI.90	Info	version number: 1.0 (0.A) date: 18.05.2022 author: Marius Rennmann, Max Schubert, Richard Poschinger, Ulrich Meier review: CCB changes: editorial corrections and changes from CCB and UNIFE review
Eu.SSI.91	Info	version number: 1.1 (0.A) date: 28.06.2023 author: Ulrich Meier, Richard Poschinger, Nicolas Poyet, André Rumbold, Max Schubert, Tobias Wothge review: Security cluster + CCB changes: Full rework for Baseline 4 Release 2
Eu.SSI.6	Head	1.2 Impressum
Eu.SSI.7	Info	Publisher: EULYNX Initiative A full list of the EULYNX Partners can be found on www.eulynx.eu/index.php/members
Eu.SSI.8	Info	Responsible for this document: EULYNX Project Management Office www.eulynx.eu
Eu.SSI.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.SSI.10	Head	1.3 Purpose
Eu.SSI.11	Info	This document describes the Standard Security Interface for the service functions related to security between the Subsystem - Security Services Platform (subsystem SSP) and the EULYNX subsystems.
Eu.SSI.29	Info	The following service functions related to security are part of the Standard Security Interface: <ul style="list-style-type: none"> • Service function Public Key Infrastructure (PKI) • Service function Security Logging (SLOG)
Eu.SSI.13	Info	This document contains general communication requirements and technical specifications (e.g. protocols and telegram definition) for the SSI (Standard Security Interface) and forms the basis for manufacturer implementation.
Eu.SSI.14	Info	This document does not specify the behaviour of the respective communication partner (e.g. the system reaction in the event of a communication failure), and in particular it does not define when which information should be sent. This behaviour is the subject of the Security services specification [Eu.Doc.121], the EULYNX Security Specification [Eu.Doc.114] and further national requirements.
Eu.SSI.15	Info	This document is intended for the following users: <ul style="list-style-type: none"> • safety authorities • infrastructure managers

ID	Type	Requirement
		<ul style="list-style-type: none"> • safety assessors • signalling system suppliers • validators • security assessors
Eu.SSI.88	Info	<p>The following statements should be considered before applying the specification:</p> <ul style="list-style-type: none"> • The security documents of the following enumeration shall be referred and used only as a complete set. <ul style="list-style-type: none"> o Eu.Doc.15 o Eu.Doc.114 o Eu.Doc.115 o Eu.Doc.116 o Eu.Doc.117 o Eu.Doc.121 • Development of the specification is based on IEC 62443 process, together with TS 50701 railway specification application suggestions. • 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. • 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). • 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.
Eu.SSI.12	Head	1.4 Applicable standards and regulations
Eu.SSI.16	Info	A list of applicable standards and regulations used in EULYNX is listed in the EULYNX Reference Document List [Eu.Doc.12].
Eu.SSI.18	Head	1.5 Applicable documents
Eu.SSI.17	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.SSI.19	Head	1.6 Terms and abbreviations
Eu.SSI.20	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9].
Eu.SSI.21	Head	1.7 Variability management
Eu.SSI.23	Info	This document is valid for the complete EULYNX System. Variability management is not used in this document.
Eu.SSI.22	Head	1.8 Definition of object types
Eu.SSI.24	Info	The following definition for object types is applied in this document:
Eu.SSI.25	Info	<ul style="list-style-type: none"> • "Req" - This denotes a mandatory requirement.
Eu.SSI.26	Info	<ul style="list-style-type: none"> • "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.
Eu.SSI.27	Info	<ul style="list-style-type: none"> • "Head" - This denotes chapter headings.
Eu.SSI.28	Head	2 Requirements
Eu.SSI.31	Head	2.1 Definition of the SSI
Eu.SSI.32	Info	The SSI requirements refer to components. The components which are required to use or provide the interfaces are defined in the Security Specification [Eu.Doc.114] and the Security Services Specification [Eu.Doc.121].
Eu.SSI.35	Head	2.1.1 Physical interface
Eu.SSI.36	Info	Physical interface requirements are defined in the Security services specification [Eu.Doc.121]
Eu.SSI.43	Head	3 SSI-XX-PKI: Public Key Infrastructure

ID	Type	Requirement
Eu.SSI.85	Info	This SSI Public Key Infrastructure interface is referenced as SSI-XX-PKI.
Eu.SSI.49	Req	If the IM decides to use CMP to implement the SSI-XX-PKI certificate management interface, the component shall use the Certificate Management Protocol (CMP) according to RFC 4210 and RFC 4211 to establish SSI-XX-PKI certificate management connections.
Eu.SSI.92	Req	If the IM decides to use CMP to implement the SSI-XX-PKI certificate management interface, the component shall transfer CMP data via HTTP (RFC 6712) to establish SSI-XX-PKI certificate management connections.
Eu.SSI.93	Req	If the IM decides to use EST to implement the SSI-XX-PKI certificate management interface, the component shall transfer certificate enrolment data via Enrollment over Secure Transport (RFC 7030) to establish SSI-XX-PKI certificate management connections.
Eu.SSI.50	Req	The component shall use a Certificate Revocation List (CRL) (RFC 5280) to establish SSI-XX-PKI certificate revocation information connections.
Eu.SSI.51	Req	The component shall transfer CRLs via HTTP (RFC 9112) to establish SSI-XX-PKI certificate revocation information connections.
Eu.SSI.53	Req	The component shall use the Open Certificate Status Protocol (RFC 6960) to establish SSI-XX-PKI certificate status connections.
Eu.SSI.56	Head	4 SSI-XX-SLOG: Security Logging
Eu.SSI.86	Info	This SSI Security Logging interface is referenced as SSI-XX-SLOG.
Eu.SSI.94	Head	4.1 Overall logging service requirements and definitions:
Eu.SSI.95	Info	This section uses the terms "log" or "logging" as data/information collected and used for monitoring, diagnostics and debugging.
Eu.SSI.96	Req	The component shall log using log entry format
Eu.SSI.827	Req	The component shall send messages containing the data of one log data point.
Eu.SSI.825	Req	The log entry format shall contain the version set to 1.
Eu.SSI.97	Req	The log entry format shall contain the data point ID
Eu.SSI.98	Req	The data point ID shall use the following structure: sec.<def1>.<def2>.<def3>....
Eu.SSI.99	Info	Example: Log requirements for security log messages for Networked Devices result in sec.net.dev where the individual data point for a packet drop is sec.net.dev.dp
Eu.SSI.100	Req	The IM shall define additional data point IDs by adding its Data Universal Numbering System (DUNS) number, 9-digits without dashes after the last structure element of the prefix.
Eu.SSI.101	Info	Example: sec.net.dev.* extended to sec.net.dev.123456789.av Security – Network – Device – Organisation: 12-345-6789 – Item: actual voltage
Eu.SSI.102	Req	The log entry format shall contain the host name of the source of log information.
Eu.SSI.103	Req	The log entry format shall contain the log level.
Eu.SSI.104	Req	The log entry format shall contain the current UTC timestamp.
Eu.SSI.828	Req	The log entry format shall contain the sequence number uniquely identifying the message in incremental order for the component.
Eu.SSI.105	Req	The log entry format shall contain defined log parameters.
Eu.SSI.106	Req	The component shall transmit the log entry as soon as the corresponding event occurs.
Eu.SSI.107	Req	The component shall transfer the log entry using the SSI interface.
Eu.SSI.108	Req	The component shall assign at least one log level to each log entry.
Eu.SSI.109	Req	The component shall assign SEC_DEBUG for the highest level of logging detail used for debugging of systems.
Eu.SSI.110	Req	The component shall assign SEC_INFO for common log entries relevant to SIEM
Eu.SSI.111	Req	The component shall assign SEC_WARN for a system warning related to security, indicating a possible (future) alert, currently not negatively affecting railway operation and its security

ID	Type	Requirement
Eu.SSI.112	Req	The component shall assign SEC_ALERT for a system alert related to security which currently negatively affects railway operation and its security
Eu.SSI.113	Req	The component shall include messages of higher log levels if a certain log level is subscribed.
Eu.SSI.114	Info	The following relation of log level sets is defined: SEC_ALERT ⊂ SEC_WARN ⊂ SEC_INFO ⊂ SEC_DEBUG
Eu.SSI.115	Req	The component shall assign the highest log level to the log entry.
Eu.SSI.116	Info	The following hierarchy of log levels exist: SEC_ALERT > SEC_WARN > SEC_INFO > SEC_DEBUG
Eu.SSI.117	Head	4.2 Generic Log Message
Eu.SSI.118	Info	The generic log message defines an abstract object representing log messages sent via the SSI-XX-SLOG interface. Mappings of the generic log message to the Syslog and OPC UA protocols are given in the subsequent sections.
Eu.SSI.119	Info	Log message are composed of a meta object and a details section specific for each log data point.
Eu.SSI.120	Info	The meta-object contains the following parameters: <ul style="list-style-type: none">• version (Version of the generic log message)• timestamp (UTC timestamp when the log message was created)• hostname (Hostname of the reporting device)• severity (Severity of the log message)• id (Log message data point id)• seq (Sequence number of the log message)
Eu.SSI.121	Info	Contents of the details section are defined for each log data point. The special parameter "text" can be included in the details section to add custom free-form text to log messages.
Eu.SSI.122	Info	The following figure depicts the generic log message with two examples:
Eu.SSI.123	Info	<p>Figure Log-Message</p> <p>Meta Object</p> <p>Syslog</p> <p>Examples</p> <p>sec.log.capw</p> <p>sec.net.dev.ndw</p> <p>level (in %)</p> <p>nic (NIC identifier)</p>
Eu.SSI.124	Req	The component shall exclude commas (",") from parameter values.

ID	Type	Requirement
Eu.SSI.125	Req	The component shall exclude equal character ("=") from parameter values.
Eu.SSI.126	Head	4.3 Generic requirements for logging protocols
Eu.SSI.832	Req	The IM shall decide if Syslog or OPC UA shall be used to transfer log data.
Eu.SSI.127	Head	4.3.1 Syslog
Eu.SSI.59	Req	If the IM decides to use Syslog to implement the SSI-XX-SLOG interface, the component shall transfer log data using Syslog via TLS (RFC 5424 and RFC 5425) to establish SSI-XX-SLOG connections.
Eu.SSI.826	Req	The component shall transfer the data point ID using the Syslog MSGID field.
Eu.SSI.128	Req	The component shall transfer parameters stringified using the Syslog MSG field.
Eu.SSI.129	Req	The component shall transfer parameters as combinations of the parameter's name and its value separated by the equal character ("=").
Eu.SSI.130	Req	The component shall transfer the name-value pairs separated by commas.
Eu.SSI.829	Req	The component shall add the sequence number using the parameter “seq” with data type UInt32.
Eu.SSI.830	Req	The component shall add the version number using the parameter “version” with data type UInt32.
Eu.SSI.131	Info	Example: Log data point for packet drop (sec.net.dev.dp): version=1,seq=1,nic=eth0,srcIP=1.2.3.4,dstIP=5.6.7.8
Eu.SSI.132	Req	The attributes "id", "timestamp", "hostname", and "severity" shall not be included in log messages.
Eu.SSI.133	Info	Those attributes will be set by Syslog specific attributes in its own message header.
Eu.SSI.134	Req	The value for Facility shall be set to 16 for all log messages.
Eu.SSI.135	Req	The component shall transfer the log level SEC_DEBUG via Syslog using severity code 7.
Eu.SSI.136	Req	The component shall transfer the log level SEC_INFO via Syslog using severity code 6.
Eu.SSI.137	Req	The component shall transfer the log level SEC_WARN via Syslog using severity code 4.
Eu.SSI.138	Req	The component shall transfer the log level SEC_ALERT via Syslog using severity code 1.
Eu.SSI.139	Head	4.3.2 OPC UA
Eu.SSI.60	Req	If the IM decides to use OPC-UA to implement the SSI-XX-SLOG interface, the component shall transfer log data using OPC-UA to establish SSI-XX-SLOG connections.
Eu.SSI.140	Req	If the security logging shall be integrated into the diagnostic OPC UA information model, the IM shall define the integration.
Eu.SSI.141	Head	4.4 Log Requirements
Eu.SSI.142	Head	4.4.1 Log Requirements for Logging Services
Eu.SSI.143	Head	4.4.1.1 Interrupted Logging Connection Detected: sec.log.interr
Eu.SSI.144	Req	If the logging connection via SSI-XX-SLOG is interrupted, the SSI-XX-SLOG Service shall log the data point ID "sec.log.interr”.
Eu.SSI.145	Req	The SSI-XX-SLOG Service shall assign the data point with ID sec.log.interr to log level SEC_WARN.
Eu.SSI.146	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter “peerIP” with data type String to data point with ID sec.log.interr.
Eu.SSI.147	Head	4.4.1.2 Outdated Logging Data Detected: sec.log.outd
Eu.SSI.148	Req	If outdated incoming logging data is detected, the SSI-XX-SLOG Service shall log the data point ID “sec.log.outd”.
Eu.SSI.149	Req	The SSI-XX-SLOG Service shall assign the data point with ID sec.log.outd to log level SEC_WARN.
Eu.SSI.150	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter “peerIP” with data type String to data point with ID sec.log.outd.

ID	Type	Requirement
Eu.SSI.151	Head	4.4.1.3 Corruption of Logging Data Detected: sec.log.corr
Eu.SSI.152	Req	If corrupted incoming logging data is detected, the SSI-XX-SLOG Service shall log the data point ID "sec.log.corr".
Eu.SSI.153	Req	The SSI-XX-SLOG Service shall assign the data point with ID sec.log.corr to log level SEC_ALERT.
Eu.SSI.154	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter "peerIP" with data type String to data point with ID sec.log.corr.
Eu.SSI.155	Req	The SSI-XX-SLOG Service shall add the last non corrupted sequence number using the parameter "seqNum" with data type UInt32 to data point with ID sec.log.cor.
Eu.SSI.156	Head	4.4.1.4 Missing Logging Data Detected: sec.log.misrcv
Eu.SSI.157	Req	If missing incoming logging data is detected, the SSI-XX-SLOG Service shall log the data point ID "sec.log.misrcv".
Eu.SSI.158	Req	The component shall assign the data point with ID sec.log.misrcv to log level SEC_ALERT.
Eu.SSI.159	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter "peerIP" with data type String to data point with ID sec.log.misrcv.
Eu.SSI.160	Req	The SSI-XX-SLOG Service shall add the last successfully received sequence number using the parameter "seqNum" with data type UInt32 to data point with ID sec.log.misrcv.
Eu.SSI.161	Head	4.4.1.5 Timestamp Mismatch: sec.log.tmis
Eu.SSI.162	Info	Log data point deleted.
Eu.SSI.163	Head	4.4.1.6 Timestamp Inconsistency Detected: sec.log.tsinc
Eu.SSI.164	Req	If an inconsistent incoming log message timestamp is detected, the SSI-XX-SLOG shall log the data point ID "sec.log.tsinc".
Eu.SSI.165	Req	The SSI-XX-SLOG shall assign the data point with ID sec.log.tsinc to log level SEC_ALERT.
Eu.SSI.166	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter "peerIP" with data type String to data point with ID sec.log.tsinc.
Eu.SSI.167	Req	The SSI-XX-SLOG Service shall add sequence number of the affected message using the parameter "seqNum" with data type UInt32 to data point with ID sec.log.tsinc.
Eu.SSI.168	Head	4.4.1.7 Data Already Received: sec.log.drcv
Eu.SSI.169	Req	If an incoming log message with an already used sequence number is received, the SSI-XX-SLOG Service shall log the data point ID "sec.log.drcv".
Eu.SSI.170	Req	The SSI-XX-SLOG Service shall assign the data point with ID sec.log.drcv to log level SEC_WARN.
Eu.SSI.171	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter "peerIP" with data type String to data point with ID sec.log.drcv.
Eu.SSI.172	Req	The SSI-XX-SLOG Service shall add sequence number of the affected message using the parameter "seqNum" with data type UInt32 to data point with ID sec.log.drcv.
Eu.SSI.173	Head	4.4.1.8 Missing Log Data Detected in Storage: sec.log.misys
Eu.SSI.174	Req	If the SSI-XX-SLOG Service detects that stored logging data is missing, the SSI-XX-SLOG Service shall log the data point ID "sec.log.misys".
Eu.SSI.175	Req	The SSI-XX-SLOG Service shall assign the data point with ID sec.log.misys to log level SEC_ALERT.
Eu.SSI.176	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter "peerIP" with data type String to data point with ID sec.log.misys.
Eu.SSI.177	Req	The SSI-XX-SLOG Service shall add the first sequence number of the missing section using the parameter "seqNumStart" with data type UInt32 to data point with ID sec.log.misys.
Eu.SSI.178	Req	The SSI-XX-SLOG Service shall add the last sequence number of the missing section using the parameter "seqNumEnd" with data type UInt32 to data point with ID sec.log.misys.
Eu.SSI.179	Head	4.4.1.9 Logging Capacity Storage Reached: sec.log.capw
Eu.SSI.180	Req	If 80%, 85%, 90%, 95%, and 100% of the log capacity is reached, the SSI-XX-SLOG Service shall log the data point ID "sec.log.capw".
Eu.SSI.181	Req	The SSI-XX-SLOG Service shall assign the data point with ID sec.log.capw to log level SEC_WARN.
Eu.SSI.182	Req	The SSI-XX-SLOG Service shall add the IP address of the logging client affected using the parameter "peerIP" with data type String to data point with ID sec.log.capw.

ID	Type	Requirement
Eu.SSI.183	Req	The SSI-XX-SLOG Service shall add the percentage of log capacity reached using the parameter "level" with data type UInt8 to data point with ID sec.log.capw.
Eu.SSI.184	Head	4.4.1.10 Logging Capacity Storage Reached Alert: sec.log.capa
Eu.SSI.185	Info	Log data point deleted.
Eu.SSI.186	Head	4.4.2 Log requirements for Networked Devices
Eu.SSI.187	Head	4.4.2.1 Packet Drop: sec.net.dev.dp
Eu.SSI.188	Req	If the component drops a packet which is not blocked by the firewall, the component shall log the data point ID "sec.net.dev.dp".
Eu.SSI.189	Req	The component shall assign the data point with ID sec.net.dev.dp to log level SEC_INFO.
Eu.SSI.190	Req	The component shall add the network interface card ID using the parameter "nic" with data type String to data point with ID sec.net.dev.dp.
Eu.SSI.191	Req	The component shall add the source IP address of the packet using the parameter "srcIP" with data type String to data point with ID sec.net.dev.dp.
Eu.SSI.192	Req	The component shall add the destination IP address of the packet using the parameter "dstIP" with data type String to data point with ID sec.net.dev.dp.
Eu.SSI.193	Head	4.4.2.2 Network Interface Card Down: sec.net.dev.ndw
Eu.SSI.194	Req	If a network interface card switches its status to down, the component shall log the data point ID "sec.net.dev.ndw".
Eu.SSI.195	Req	The component shall assign the data point with ID sec.net.dev.ndw to log level SEC_INFO.
Eu.SSI.196	Req	The component shall add the network interface card ID using the parameter "nic" with data type String to data point with ID sec.net.dev.ndw.
Eu.SSI.197	Head	4.4.2.3 Network Interface Card Up: sec.net.dev.nup
Eu.SSI.198	Req	If a network interface card switches its status to up, the component shall log the data point ID "sec.net.dev.nup".
Eu.SSI.199	Req	The component shall assign the data point with ID sec.net.dev.nup to log level SEC_INFO.
Eu.SSI.200	Req	The component shall add the network interface card ID using the parameter "nic" with data type String to data point with ID sec.net.dev.nup.
Eu.SSI.201	Head	4.4.2.4 TCP Reset Segment Received: sec.net.dev.tcprst
Eu.SSI.202	Req	If a TCP reset segment is received, the component shall log the data point ID "sec.net.dev.tcprst".
Eu.SSI.203	Req	The component shall assign the data point with ID sec.net.dev.tcprst to log level SEC_WARN.
Eu.SSI.204	Req	The component shall add the network interface card ID using the parameter "nic" with data type String to data point with ID sec.net.dev.tcprst.
Eu.SSI.205	Req	The component shall add the source IP address of the packet using the parameter "srcIP" with data type String to data point with ID sec.net.dev.tcprst.
Eu.SSI.206	Req	The component shall add the destination IP address of the packet using the parameter "dstIP" with data type String to data point with ID sec.net.dev.tcprst.
Eu.SSI.207	Head	4.4.2.5 Martian Packet Received: sec.net.dev.mp
Eu.SSI.208	Req	If a packet not matching the permitted source subnets is received, the component shall log the data point ID "sec.net.dev.mp".
Eu.SSI.209	Req	The component shall assign the data point with ID sec.net.dev.mp to log level SEC_ALERT
Eu.SSI.210	Req	The component shall add the network interface card ID using the parameter "nic" with data type String to data point with ID sec.net.dev.mp.
Eu.SSI.211	Req	The component shall add the source IP address of the packet using the parameter "srcIP" with data type String to data point with ID sec.net.dev.mp.
Eu.SSI.212	Req	The component shall add the destination IP address of the packet using the parameter "dstIP" with data type String to data point with ID sec.net.dev.mp.
Eu.SSI.213	Head	4.4.2.6 New DHCP Lease Requested: sec.net.dev.ndreq
Eu.SSI.214	Req	If a NIC requests a new DHCP lease, the component shall log the data point ID "sec.net.dev.ndreq".

ID	Type	Requirement
Eu.SSI.215	Info	The data point with ID sec.net.dev.ndreq shall also be logged if a DHCP lease is renewed.
Eu.SSI.216	Req	The component shall assign the data point with ID sec.net.dev.ndreq to log level SEC_INFO.
Eu.SSI.217	Req	The component shall add the network interface card ID using the parameter “nic” with data type String to data point with ID sec.net.dev.ndreq.
Eu.SSI.218	Head	4.4.2.7 DHCP New IP Received: sec.net.dev.ndesp
Eu.SSI.219	Req	If a new IP address is received via DHCP, the component shall log the data point ID “sec.net.dev.ndesp”.
Eu.SSI.220	Req	The component shall assign the data point with ID sec.net.dev.ndesp to log level SEC_INFO.
Eu.SSI.221	Req	The component shall add the network interface card ID using the parameter “nic” with data type String to data point with ID sec.net.dev.ndesp.
Eu.SSI.222	Req	The component shall add the new IP address received via DHCP using the parameter “newIP” with data type String to data point with ID sec.net.dev.ndesp.
Eu.SSI.223	Req	The component shall add the old IP used by the NIC using the parameter “oldIP” with data type String to data point with ID sec.net.dev.ndesp.
Eu.SSI.224	Head	4.4.2.8 Firewall Warnings and Blocked Connections: sec.net.dev.fwbc
Eu.SSI.225	Info	Log data point deleted.
Eu.SSI.226	Head	4.4.2.9 Firewall Warning: sec.net.dev.fww
Eu.SSI.227	Req	If a warning by the component's firewall is emitted, the component shall log the data point ID “sec.net.dev.fww”.
Eu.SSI.228	Req	The component shall assign the data point with ID sec.net.dev.fww to log level SEC_WARN.
Eu.SSI.229	Req	The component shall add the warning message of the internal firewall using the parameter “warnMsg” with data type String to data point with ID sec.net.dev.fww.
Eu.SSI.230	Head	4.4.2.10 Change in Cabling Detected: sec.net.dev.chcbl
Eu.SSI.231	Req	If the change of cabling is detected at a NIC, the component shall log the data point ID “sec.net.dev.chcbl”.
Eu.SSI.232	Req	The component shall assign the data point with ID sec.net.dev.chcbl to log level SEC_ALERT.
Eu.SSI.233	Req	The component shall add the network interface card ID using the parameter “nic” with data type String to data point with ID sec.net.dev.chcbl.
Eu.SSI.234	Head	4.4.2.11 Detect Physical Port Speed Change: sec.net.dev.chspd
Eu.SSI.235	Req	If a change in the physical port speed is detected, the component shall log the data point ID “sec.net.dev.chspd”.
Eu.SSI.236	Req	The component shall assign the data point with ID sec.net.dev.chspd to log level SEC_INFO.
Eu.SSI.237	Req	The component shall add the network interface card ID using the parameter “nic” with data type String to data point with ID sec.net.dev.chspd.
Eu.SSI.238	Req	The component shall add the old speed in Bit/s using the parameter “oldSpd” with data type UInt64 to data point with ID sec.net.dev.chspd.
Eu.SSI.239	Req	The component shall add the new speed in Bit/s using the parameter “newSpd” with data type UInt64 to data point with ID sec.net.dev.chspd.
Eu.SSI.240	Head	4.4.2.12 Connection Attempt to Management Port: sec.net.dev.camp
Eu.SSI.241	Req	If a connection attempt to the management port is detected, the component shall log the data point ID “sec.net.dev.camp”.
Eu.SSI.242	Req	The component shall assign the data point with ID sec.net.dev.camp to log level SEC_ALERT.
Eu.SSI.243	Head	4.4.2.13 Too Many Open Sockets: sec.net.dev.tmc
Eu.SSI.244	Req	If too many open sockets are detected, the component shall log the data point ID “sec.net.dev.tmc”.
Eu.SSI.245	Req	The component shall assign the data point with ID sec.net.dev.tmc to log level SEC_ALERT.
Eu.SSI.246	Head	4.4.2.14 Disabled TCP or UDP Port Activated: sec.net.dev.dlprta

ID	Type	Requirement
Eu.SSI.247	Req	If a TCP or UDP port not used by a permitted network service is activated, the component shall log the data point ID "sec.net.dev.dlprta".
Eu.SSI.248	Req	The component shall assign the data point with ID sec.net.dev.dlprta to log level SEC_ALERT.
Eu.SSI.249	Req	The component shall add the TCP or UDP port number using the parameter "port" with data type UInt16 to data point with ID sec.net.dev.dlprta.
Eu.SSI.250	Req	The component shall add the service name using the parameter "service" with data type String to data point with ID sec.net.dev.dlprta.
Eu.SSI.251	Head	4.4.2.15 Internal Errors: sec.net.dev.ierr
Eu.SSI.252	Req	If an internal error not handled by other error messages is detected, the component shall log the data point ID "sec.net.dev.ierr".
Eu.SSI.253	Req	The component shall assign the data point with ID sec.net.dev.ierr to log level SEC_ALERT.
Eu.SSI.254	Req	The component shall add the error description using the parameter "errorMsg" with data type String to data point with ID sec.net.dev.ierr.
Eu.SSI.255	Head	4.4.2.16 Internal Warning: sec.net.dev.iwarn
Eu.SSI.256	Req	If an internal warning not handled by other messages is detected, the component shall log the data point ID "sec.net.dev.iwarn".
Eu.SSI.257	Req	The component shall assign the data point with ID sec.net.dev.iwarn to log level SEC_WARN.
Eu.SSI.258	Req	The component shall add the error description using the parameter "warnMsg" with data type String to data point with ID sec.net.dev.iwarn.
Eu.SSI.259	Head	4.4.2.17 Shutdown due to Security Error: sec.net.dev.isec
Eu.SSI.260	Req	If the component is shutdown due to a security error, the component shall log the data point ID "sec.net.dev.isec".
Eu.SSI.261	Req	The component shall assign the data point with ID sec.net.dev.isec to log level SEC_ALERT.
Eu.SSI.262	Req	The component shall add the error description using the parameter "errorMsg" with data type String to data point with ID sec.net.dev.isec.
Eu.SSI.263	Head	4.4.2.18 Packet Blocked: sec.net.dev.caprt
Eu.SSI.264	Req	If a packet is blocked by the components firewall, the component shall log the data point ID "sec.net.dev.caprt".
Eu.SSI.265	Req	The component shall assign the data point with ID sec.net.dev.caprt to log level SEC_WARN.
Eu.SSI.266	Req	The component shall add the source IP address of the packet using the parameter "srcIP" with data type String to data point with ID sec.net.dev.caprt.
Eu.SSI.267	Req	The component shall add the destination IP address of the packet using the parameter "dstIP" with data type String to data point with ID sec.net.dev.caprt.
Eu.SSI.268	Req	The component shall add the source port of the packet using the parameter "srcPort" with data type UInt16 to data point with ID sec.net.dev.caprt.
Eu.SSI.269	Req	The component shall add the destination port of the packet using the parameter "dstPort" with data type UInt16 to data point with ID sec.net.dev.caprt.
Eu.SSI.270	Req	The component shall add the layer protocol detected on the highest network layer of the packet using the parameter "proto" with data type String to data point with ID sec.net.dev.caprt.
Eu.SSI.271	Head	4.4.2.19 Authentication failed: sec.net.dev.caauth
Eu.SSI.272	Req	If an authentication procedure fails which is not TLS or OPC-UA or NAC based, the component shall log the data point ID "sec.net.dev.caauth".
Eu.SSI.273	Req	The component shall assign the data point with ID sec.net.dev.caauth to log level SEC_ALERT.
Eu.SSI.274	Req	The component shall add the affected service using the parameter "service" with data type String to data point with ID sec.net.dev.caauth.
Eu.SSI.275	Req	The component shall add the affected authenticated user using the parameter "user" with data type String to data point with ID sec.net.dev.caauth.
Eu.SSI.276	Head	4.4.3 Log requirements for Network Security Components
Eu.SSI.277	Head	4.4.3.1 Network Security Component Warning: sec.net.sec.warn
Eu.SSI.278	Req	If the network security component detects an issue, the network security component shall log the data point ID "sec.net.sec.warn".

ID	Type	Requirement
Eu.SSI.279	Req	The network security component shall assign the data point with ID sec.net.sec.warn to log level SEC_WARN.
Eu.SSI.280	Req	The network security component shall add the error description using the parameter "warnMsg" with data type String to data point with ID sec.net.sec.warn.
Eu.SSI.281	Head	4.4.3.2 Firewall Blocked Connection: sec.net.sec.blc
Eu.SSI.282	Req	If the firewall blocks a connection or packet, the firewall shall log the data point ID "sec.net.sec.blc".
Eu.SSI.283	Req	The firewall shall assign the data point with ID sec.net.sec.blc to log level SEC_WARN.
Eu.SSI.284	Req	The firewall shall add the source IP address of the packet using the parameter "srcIP" with data type String to data point with ID sec.net.sec.blc.
Eu.SSI.285	Req	The firewall shall add the destination IP address of the packet using the parameter "dstIP" with data type String to data point with ID sec.net.sec.blc.
Eu.SSI.286	Req	The firewall shall add the source port of the packet using the parameter "srcPort" with data type UInt16 to data point with ID sec.net.sec.blc.
Eu.SSI.287	Req	The firewall shall add the destination port of the packet using the parameter "dstPort" with data type UInt16 to data point with ID sec.net.sec.blc.
Eu.SSI.288	Req	The firewall shall add the layer protocol detected on the highest network layer of the packet using the parameter "proto" with data type String to data point with ID sec.net.sec.blc.
Eu.SSI.289	Head	4.4.3.3 Denial of Service Detected: sec.net.sec.dos
Eu.SSI.290	Req	If the network security component detects a denial of service attack, the network security component shall log the data point ID "sec.net.sec.dos".
Eu.SSI.291	Req	The network security component shall assign the data point with ID sec.net.sec.dos to log level SEC_ALERT.
Eu.SSI.292	Req	If the network security component identities a target IP subnet, the component shall add the target IP subnet of the denial of service attack using the parameter "targetIPsub" with data type String in CIDR format to data point with ID sec.net.sec.dos.
Eu.SSI.293	Head	4.4.3.4 Malicious Content: sec.net.sec.mc
Eu.SSI.294	Req	If the network security component detects malicious content in a packet, the component shall log the data point ID "sec.net.sec.mc".
Eu.SSI.295	Req	The network security component shall assign the data point with ID sec.net.sec.mc to log level SEC_ALERT.
Eu.SSI.296	Req	The firewall shall add the source IP address of the packet using the parameter "srcIP" with data type String to data point with ID sec.net.sec.mc.
Eu.SSI.297	Req	The firewall shall add the destination IP address of the packet using the parameter "dstIP" with data type String to data point with ID sec.net.sec.mc.
Eu.SSI.298	Req	The firewall shall add the source port of the packet using the parameter "srcPort" with data type UInt16 to data point with ID sec.net.sec.mc.
Eu.SSI.299	Req	The firewall shall add the destination port of the packet using the parameter "dstPort" with data type UInt16 to data point with ID sec.net.sec.mc.
Eu.SSI.300	Req	The firewall shall add the layer protocol detected on the highest network layer of the packet using the parameter "proto" with data type String to data point with ID sec.net.sec.mc.
Eu.SSI.301	Head	4.4.4 Log requirements for RaSTA
Eu.SSI.302	Head	4.4.4.1 RaSTA Connection Terminated due to Sequence Error: sec.rasta.tdse
Eu.SSI.303	Req	If the component terminates a RaSTA connection due to a sequence error, the component shall log the data point ID "sec.rasta.tdse".
Eu.SSI.304	Req	The component shall assign the data point with ID sec.rasta.tdse to log level SEC_WARN.
Eu.SSI.305	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.tdse.
Eu.SSI.306	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.tdse.
Eu.SSI.307	Req	The component shall add the last valid sequence number of the affected channel using the parameter "rastaSeqNum" with data type UInt32 to data point with ID sec.rasta.tdse.
Eu.SSI.308	Head	4.4.4.2 RaSTA Payload: sec.rasta.pct
Eu.SSI.309	Info	Log data point deleted. SDI might be used to transfer RaSTA payload for debugging purposes.
Eu.SSI.310	Head	4.4.4.3 RaSTA Connection Failed: sec.rasta.fce

ID	Type	Requirement
Eu.SSI.311	Req	If the component detects a failed RaSTA connection, the component shall log the data point ID "sec.rasta.fce".
Eu.SSI.312	Req	The component shall assign the data point with ID sec.rasta.fce to log level SEC_WARN.
Eu.SSI.313	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.fce.
Eu.SSI.314	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.fce.
Eu.SSI.315	Head	4.4.4.4 RaSTA Redundancy Channel Connection Established: sec.rasta.rcest
Eu.SSI.316	Req	If the component established a RaSTA redundancy channel, the component shall log the data point ID "sec.rasta.rcest".
Eu.SSI.317	Req	The component shall assign the data point with ID sec.rasta.rcest to log level SEC_INFO.
Eu.SSI.318	Req	The component shall add the remote IP of the affected channel using the parameter "remIP" with data type String to data point with ID sec.rasta.rcest.
Eu.SSI.319	Req	The component shall add the local IP of the affected channel using the parameter "locIP" with data type String to data point with ID sec.rasta.rcest.
Eu.SSI.320	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.rcest.
Eu.SSI.321	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.rcest.
Eu.SSI.322	Head	4.4.4.5 RaSTA Safety Channel Connection Established: sec.rasta.sacest
Eu.SSI.323	Req	If the component established a RaSTA safety channel, the component shall log the data point ID "sec.rasta.sacest".
Eu.SSI.324	Req	The component shall assign the data point with ID sec.rasta.sacest to log level SEC_INFO.
Eu.SSI.325	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.sacest.
Eu.SSI.326	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.sacest.
Eu.SSI.327	Head	4.4.4.6 RaSTA Channel A Connection Established: sec.rasta.cra
Eu.SSI.328	Info	Log data point replaced by sec.rasta.rcest.
Eu.SSI.329	Head	4.4.4.7 RaSTA Channel B Connection Established: sec.rasta.crb
Eu.SSI.330	Info	Log data point replaced by sec.rasta.rcest.
Eu.SSI.331	Head	4.4.4.8 RaSTA Channel C Connection Established: sec.rasta.crc
Eu.SSI.332	Info	Log data point replaced by sec.rasta.rcest.
Eu.SSI.333	Head	4.4.4.9 RaSTA Redundancy Channel Connection Lost: sec.rasta.lrc
Eu.SSI.334	Req	If the component loses connection via a RaSTA redundancy channel, the component shall log the data point ID "sec.rasta.lrc".
Eu.SSI.335	Req	The component shall assign the data point with ID sec.rasta.lrc to log level SEC_WARN.
Eu.SSI.336	Req	The component shall add the remote IP of the affected channel using the parameter "remIP" with data type String to data point with ID sec.rasta.lrc.
Eu.SSI.337	Req	The component shall add the local IP of the affected channel using the parameter "locIP" with data type String to data point with ID sec.rasta.lrc.
Eu.SSI.338	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.lrc.
Eu.SSI.339	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.lrc.
Eu.SSI.340	Head	4.4.4.10 RaSTA Redundany Channel A Lost: sec.rasta.lrca
Eu.SSI.341	Info	Log data point replaced by sec.rasta.lrc.
Eu.SSI.342	Head	4.4.4.11 RaSTA Redundany Channel B Lost: sec.rasta.lrcb

ID	Type	Requirement
Eu.SSI.343	Info	Log data point replaced by sec.rasta.lrc.
Eu.SSI.344	Head	4.4.4.12 RaSTA Redundany Channel C Lost: sec.log.lrcc
Eu.SSI.345	Info	Log data point replaced by sec.rasta.lrc.
Eu.SSI.346	Head	4.4.4.13 RaSTA Heartbeat Missing: sec.rasta.hbm
Eu.SSI.347	Req	If the component detects a missing RaSTA heartbeat, the component shall log the data point ID “sec.rasta.hbm”.
Eu.SSI.348	Req	The component shall assign the data point with ID sec.rasta.hbm to log level SEC_WARN.
Eu.SSI.349	Req	The component shall add the RaSTA sender ID using the parameter “rastaSdr” with data type UInt32 to data point with ID sec.rasta.hbm.
Eu.SSI.350	Req	The component shall add the RaSTA receiver ID using the parameter “rastaRcv” with data type UInt32 to data point with ID sec.rasta.hbm.
Eu.SSI.351	Req	The component shall add the last valid sequence number of the affected channel using the parameter “rastaSeqNum” with data type UInt32 to data point with ID sec.rasta.hbm.
Eu.SSI.352	Head	4.4.4.14 RaSTA Resend Triggered: sec.rasta.rst
Eu.SSI.353	Req	If the component sends a RaSTA resend packet, the component shall log the data point ID “sec.rasta.rst”.
Eu.SSI.354	Req	The component shall assign the data point with ID sec.rasta.rst to log level SEC_INFO.
Eu.SSI.355	Req	The component shall add the RaSTA sender ID using the parameter “rastaSdr” with data type UInt32 to data point with ID sec.rasta.rst.
Eu.SSI.356	Req	The component shall add the RaSTA receiver ID using the parameter “rastaRcv” with data type UInt32 to data point with ID sec.rasta.rst.
Eu.SSI.357	Req	The component shall add the last valid sequence number of the affected channel using the parameter “rastaSeqNum” with data type UInt32 to data point with ID sec.rasta.rst.
Eu.SSI.358	Head	4.4.4.15 RaSTA Connection Request: sec.rasta.crd
Eu.SSI.359	Req	If the component send a RaSTA connection request, the component shall log the data point ID “sec.rasta.crd”.
Eu.SSI.360	Req	The component shall assign the data point with ID sec.rasta.crd to log level SEC_INFO.
Eu.SSI.361	Req	The component shall add the RaSTA sender ID using the parameter “rastaSdr” with data type UInt32 to data point with ID sec.rasta.crd.
Eu.SSI.362	Req	The component shall add the RaSTA receiver ID using the parameter “rastaRcv” with data type UInt32 to data point with ID sec.rasta.crd.
Eu.SSI.363	Head	4.4.4.16 RaSTA Termination Request: sec.rasta.rctr
Eu.SSI.364	Req	If the component send a RaSTA termination request, the component shall log the data point ID “sec.rasta.rctr”.
Eu.SSI.365	Req	The component shall assign the data point with ID sec.rasta.rctr to log level SEC_INFO.
Eu.SSI.366	Req	The component shall add the RaSTA sender ID using the parameter “rastaSdr” with data type UInt32 to data point with ID sec.rasta.rctr.
Eu.SSI.367	Req	The component shall add the RaSTA receiver ID using the parameter “rastaRcv” with data type UInt32 to data point with ID sec.rasta.rctr.
Eu.SSI.368	Req	The component shall add the RaSTA termination reason code using the parameter “rastaTC” with data type UInt16 to data point with ID sec.rasta.rctr.
Eu.SSI.369	Req	The component shall add the RaSTA termination detail reason code using the parameter “rastaTCd” with data type UInt16 to data point with ID sec.rasta.rctr.
Eu.SSI.370	Req	The component shall add the last valid sequence number of the affected channel using the parameter “rastaSeqNum” with data type UInt32 to data point with ID sec.rasta.rctr.
Eu.SSI.371	Head	4.4.4.17 RaSTA Connection Terminated: sec.rasta.rct
Eu.SSI.372	Req	If the component terminates the RaSTA connection, the component shall log the data point ID “sec.rasta.rct”.
Eu.SSI.373	Req	The component shall assign the data point with ID sec.rasta.rct to log level SEC_INFO.
Eu.SSI.374	Req	The component shall add the RaSTA sender ID using the parameter “rastaSdr” with data type UInt32 to data point with ID sec.rasta.rct.

ID	Type	Requirement
Eu.SSI.375	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.rct.
Eu.SSI.376	Req	The component shall add the RaSTA termination reason code using the parameter "rastaTC" with data type UInt16 to data point with ID sec.rasta.rct.
Eu.SSI.377	Req	The component shall add the RaSTA termination detail reason code using the parameter "rastaTCd" with data type UInt16 to data point with ID sec.rasta.rct.
Eu.SSI.378	Req	The component shall add the last valid sequence number of the affected channel using the parameter "rastaSeqNum" with data type UInt32 to data point with ID sec.rasta.rct.
Eu.SSI.379	Head	4.4.4.18 RaSTA Redundancy Layer Error: sec.rasta.emr
Eu.SSI.380	Req	If the component detects an error on the redundancy layer, the component shall log the data point ID "sec.rasta.emr".
Eu.SSI.381	Req	The component shall assign the data point with ID sec.rasta.emr to log level SEC_WARN.
Eu.SSI.382	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.emr.
Eu.SSI.383	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.emr.
Eu.SSI.384	Req	The component shall add the error message using the parameter "errorMsg" with data type String to data point with ID sec.rasta.emr.
Eu.SSI.385	Req	The component shall add the remote IP of the affected channel using the parameter "remIP" with data type String to data point with ID sec.rasta.emr.
Eu.SSI.386	Req	The component shall add the local IP of the affected channel using the parameter "locIP" with data type String to data point with ID sec.rasta.emr.
Eu.SSI.387	Req	The component shall add the last valid sequence number of the affected channel using the parameter "rastaSeqNum" with data type UInt32 to data point with ID sec.rasta.emr.
Eu.SSI.388	Head	4.4.4.19 RaSTA Safety Layer Error: sec.rasta.ems
Eu.SSI.389	Req	If the component detects an error on the safety layer, the component shall log the data point ID "sec.rasta.ems".
Eu.SSI.390	Req	The component shall assign the data point with ID sec.rasta.ems to log level SEC_WARN.
Eu.SSI.391	Req	The component shall add the RaSTA sender ID using the parameter "rastaSdr" with data type UInt32 to data point with ID sec.rasta.ems.
Eu.SSI.392	Req	The component shall add the RaSTA receiver ID using the parameter "rastaRcv" with data type UInt32 to data point with ID sec.rasta.ems.
Eu.SSI.393	Req	The component shall add the error message using the parameter "errorMsg" with data type String to data point with ID sec.rasta.ems.
Eu.SSI.394	Req	The component shall add the last valid sequence number of the affected channel using the parameter "rastaSeqNum" with data type UInt32 to data point with ID sec.rasta.ems.
Eu.SSI.395	Head	4.4.4.20 RaSTA Transport Layer Error: sec.rasta.emta
Eu.SSI.396	Req	If the component detects a RaSTA error on the transport layer and this error is not covered by TLS log data points, the component shall log the data point ID "sec.rasta.emta".
Eu.SSI.397	Req	The component shall assign the data point with ID sec.rasta.emta to log level SEC_WARN.
Eu.SSI.398	Req	The component shall add the error message using the parameter "errorMsg" with data type String to data point with ID sec.rasta.emta.
Eu.SSI.399	Req	The component shall add the remote IP of the affected channel using the parameter "remIP" with data type String to data point with ID sec.rasta.emta.
Eu.SSI.400	Req	The component shall add the local IP of the affected channel using the parameter "locIP" with data type String to data point with ID sec.rasta.emta.
Eu.SSI.401	Req	The component shall add the last valid sequence number of the affected channel using the parameter "rastaSeqNum" with data type UInt32 to data point with ID sec.rasta.emta.
Eu.SSI.402	Head	4.4.5 Log requirements for OPC UA
Eu.SSI.403	Head	4.4.5.1 Binary Secure Conversation Requested: sec.opcua.bscr
Eu.SSI.404	Req	If the component requests an OPC UA Binary Secure Conversation, the component shall log the data point ID "sec.opcua.bscr".
Eu.SSI.405	Req	The component shall assign the data point with ID sec.opcua.bscr to log level SEC_INFO.
Eu.SSI.406	Req	The component shall add the local IP address of the connection using the parameter "locIP" with data type String to data point with ID sec.opcua.bscr.

ID	Type	Requirement
Eu.SSI.407	Req	The component shall add the remote IP address of the connection using the parameter "remoteIP" with data type String to data point with ID sec.opcua.bscr.
Eu.SSI.408	Head	4.4.5.2 Binary Secure Conversation Established: sec.opcua.bsce
Eu.SSI.409	Req	If the component established an OPC UA Binary Secure Conversation, the component shall log the data point ID "sec.opcua.bsce".
Eu.SSI.410	Req	The component shall assign the data point with ID sec.opcua.bsce to log level SEC_INFO.
Eu.SSI.411	Req	The component shall add the local IP address of the connection using the parameter "locIP" with data type String to data point with ID sec.opcua.bsce.
Eu.SSI.412	Req	The component shall add the remote IP address of the connection using the parameter "remoteIP" with data type String to data point with ID sec.opcua.bsce.
Eu.SSI.413	Head	4.4.5.3 Binary Secure Conversation Connection Establishment Failed: sec.opcua.bscf
Eu.SSI.414	Req	If the component failed to establish an OPC UA Binary Secure Conversation, the component shall log the data point ID "sec.opcua.bscf".
Eu.SSI.415	Req	The component shall assign the data point with ID sec.opcua.bscf to log level SEC_INFO.
Eu.SSI.416	Req	The component shall add the local IP address of the connection using the parameter "locIP" with data type String to data point with ID sec.opcua.bscf.
Eu.SSI.417	Req	The component shall add the remote IP address of the connection using the parameter "remoteIP" with data type String to data point with ID sec.opcua.bscf.
Eu.SSI.418	Head	4.4.5.4 Binary Secure Conversation Connection Error: sec.opcua.embsc
Eu.SSI.419	Req	If the component detects an error in an OPC UA Binary Secure Conversation, the component shall log the data point ID "sec.opcua.embsc".
Eu.SSI.420	Req	The component shall assign the data point with ID sec.opcua.embsc to log level SEC_WARN.
Eu.SSI.421	Req	The component shall add the local IP address of the connection using the parameter "locIP" with data type String to data point with ID sec.opcua.embsc.
Eu.SSI.422	Req	The component shall add the remote IP address of the connection using the parameter "remoteIP" with data type String to data point with ID sec.opcua.embsc.
Eu.SSI.423	Req	The component shall add OPC UA error description using the parameter "errorMsg" with data type String to data point with ID sec.opcua.embsc.
Eu.SSI.424	Head	4.4.6 Log requirements for Network Access Control
Eu.SSI.425	Info	NAC messages regarding EAP-TLS authentication are covered by sec.tls.*
Eu.SSI.426	Head	4.4.6.1 NAC Disconnect or Connect: sec.net.nac.popi
Eu.SSI.427	Info	Log data point deleted.
Eu.SSI.428	Head	4.4.6.2 NAC Invalid Certificate: sec.net.nac.cic
Eu.SSI.429	Req	If the SCS detects a connection attempt via NAC with an invalid certificate, the component shall log the data point ID "sec.net.nac.cic".
Eu.SSI.430	Req	The component shall assign the data point with ID sec.net.nac.cic to log level SEC_ALERT.
Eu.SSI.431	Req	The component shall add the IP address of the connecting component using "conIP" with data type String to data point with ID sec.net.nac.cic.
Eu.SSI.432	Head	4.4.6.3 Network Access Granted: sec.net.nac.cvc
Eu.SSI.433	Req	If the SCS grants access to a component as result of a valid NAC request, the component shall log the data point ID "sec.net.nac.cvc".
Eu.SSI.434	Req	The component shall assign the data point with ID sec.net.nac.cvc to log level SEC_INFO.
Eu.SSI.435	Req	The component shall add the IP address of the connecting component using "conIP" with data type String to data point with ID sec.net.nac.cvc.
Eu.SSI.436	Head	4.4.6.4 NAC Network Access Timeout: sec.net.nac.rvk
Eu.SSI.437	Req	If the SCS revokes the network access due to network downtime, the component shall log the data point ID "sec.net.nac.rvk".
Eu.SSI.438	Req	The component shall assign the data point with ID sec.net.nac.rvk to log level SEC_WARN.

ID	Type	Requirement
Eu.SSI.439	Req	The component shall add the IP address of the connecting component using “conIP” with data type String to data point with ID sec.net.nac.rvk.
Eu.SSI.440	Head	4.4.7 Log requirements for TLS
Eu.SSI.441	Head	4.4.7.1 TLS Dropped Connection - Sequence Error: sec.tls.dcse
Eu.SSI.442	Req	If the component drops a connection due to a sequence error in TLS, the component shall log the data point ID “sec.tls.dcse”.
Eu.SSI.443	Req	The component shall assign the data point with ID sec.tls.dcse to log level SEC_INFO.
Eu.SSI.444	Req	The component shall add the local IP address of the TLS connection using the parameter “locIP” with data type String to data point with ID sec.tls.dcse.
Eu.SSI.445	Req	The component shall add the remote IP address of the TLS connection using the parameter “remoteIP” with data type String to data point with ID sec.tls.dcse.
Eu.SSI.446	Req	The component shall add the local port of the TLS connection using the parameter “locPort” with data type UInt16 to data point with ID sec.tls.dcse.
Eu.SSI.447	Req	The component shall add the remote port of the TLS connection using the parameter “remotePort” with data type UInt16 to data point with ID sec.tls.dcse.
Eu.SSI.448	Head	4.4.7.2 TLS Connection Attempt with Invalid Certificate: sec.tls.cic
Eu.SSI.449	Req	If the component detects a connection attempt with an invalid TLS certificate and if this case is not covered by other TLS log messages, the component shall log the data point ID “sec.tls.cic”.
Eu.SSI.450	Req	The component shall assign the data point with ID sec.tls.cic to log level SEC_ALERT.
Eu.SSI.451	Req	The component shall add the local IP address of the TLS connection using the parameter “locIP” with data type String to data point with ID sec.tls.cic.
Eu.SSI.452	Req	The component shall add the remote IP address of the TLS connection using the parameter “remoteIP” with data type String to data point with ID sec.tls.cic.
Eu.SSI.453	Req	The component shall add the local port of the TLS connection using the parameter “locPort” with data type UInt16 to data point with ID sec.tls.cic.
Eu.SSI.454	Req	The component shall add the remote port of the TLS connection using the parameter “remotePort” with data type UInt16 to data point with ID sec.tls.cic.
Eu.SSI.455	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter “certCN” with data type String to data point with ID sec.tls.cic.
Eu.SSI.456	Head	4.4.7.3 TLS Invalid Certificate: Rid field invalid: sec.tls.cicrid
Eu.SSI.457	Info	Log data point deleted.
Eu.SSI.458	Head	4.4.7.4 TLS Connection Attempt with Invalid Certificate (Root not trusted): sec.tls.cicrc
Eu.SSI.459	Req	If the component detects a connection attempt with an invalid TLS certificate due to an untrusted root , the component shall log the data point ID “sec.tls.cicrc”.
Eu.SSI.460	Req	The component shall assign the data point with ID sec.tls.cicrc to log level SEC_ALERT.
Eu.SSI.461	Req	The component shall add the local IP address of the TLS connection using the parameter “locIP” with data type String to data point with ID sec.tls.cicrc.
Eu.SSI.462	Req	The component shall add the remote IP address of the TLS connection using the parameter “remoteIP” with data type String to data point with ID sec.tls.cicrc.
Eu.SSI.463	Req	The component shall add the local port of the TLS connection using the parameter “locPort” with data type UInt16 to data point with ID sec.tls.cicrc.
Eu.SSI.464	Req	The component shall add the remote port of the TLS connection using the parameter “remotePort” with data type UInt16 to data point with ID sec.tls.cicrc.
Eu.SSI.465	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter “certCN” with data type String to data point with ID sec.tls.cicrc.
Eu.SSI.466	Head	4.4.7.5 TLS Connection Attempt with Invalid Certificate (Certificate Expired): sec.tls.cicte
Eu.SSI.467	Req	If the component detects a connection attempt with an expired TLS certificate, the component shall log the data point ID “sec.tls.cicte”.
Eu.SSI.468	Req	The component shall assign the data point with ID sec.tls.cicte to log level SEC_WARN.
Eu.SSI.469	Req	The component shall add the local IP address of the TLS connection using the parameter “locIP” with data type String to data point with ID sec.tls.cicte.
Eu.SSI.470	Req	The component shall add the remote IP address of the TLS connection using the parameter “remoteIP” with data type String to data point with ID sec.tls.cicte.

ID	Type	Requirement
Eu.SSI.471	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cicte.
Eu.SSI.472	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cicte.
Eu.SSI.473	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter "certCN" with data type String to data point with ID sec.tls.cicte.
Eu.SSI.474	Req	The component shall add the certificate expiry date (not after) of the TLS certificate used by the connecting party using the parameter "certExp" with data type Timestamp to data point with ID sec.tls.cicte.
Eu.SSI.475	Head	4.4.7.6 TLS Connection Attempt with Certificate not Authorised for Connection: sec.tls.cicna
Eu.SSI.476	Req	If the component detects a connection attempt with an valid TLS certificate which is not authorised for the connection , the component shall log the data point ID "sec.tls.cicna".
Eu.SSI.477	Req	The component shall assign the data point with ID sec.tls.cicna to log level SEC_ALERT.
Eu.SSI.478	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.cicna.
Eu.SSI.479	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.cicna.
Eu.SSI.480	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cicna.
Eu.SSI.481	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cicna.
Eu.SSI.482	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter "certCN" with data type String to data point with ID sec.tls.cicna.
Eu.SSI.483	Head	4.4.7.7 TLS Connection Established: sec.tls.cvc
Eu.SSI.484	Req	If the component successfully established an authenticated and authorised connection, the component shall log the data point ID "sec.tls.cvc".
Eu.SSI.485	Req	The component shall assign the data point with ID sec.tls.cvc to log level SEC_INFO.
Eu.SSI.486	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.cvc.
Eu.SSI.487	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.cvc.
Eu.SSI.488	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cvc.
Eu.SSI.489	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cvc.
Eu.SSI.490	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter "certCN" with data type String to data point with ID sec.tls.cvc.
Eu.SSI.491	Head	4.4.7.8 Dropped TLS due to Transport Layer Error: sec.tls.dcte
Eu.SSI.492	Req	If the component detects a TLS connection drop due to an error on the transport layer, the component shall log the data point ID "sec.tls.dcte".
Eu.SSI.493	Req	The component shall assign the data point with ID sec.tls.dcte to log level SEC_INFO.
Eu.SSI.494	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.dcte.
Eu.SSI.495	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.dcte.
Eu.SSI.496	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.dcte.
Eu.SSI.497	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.dcte.
Eu.SSI.498	Req	The component shall add the transport layer error description using the parameter "errorMsg" with data type String to data point with ID sec.tls.dcte.
Eu.SSI.499	Head	4.4.7.9 TLS Failed to Establish Connection: sec.tls.cf
Eu.SSI.500	Req	If the component fails to establish an TLS connection and if this case is not covered by other TLS log messages , the component shall log the data point ID "sec.tls.cf".
Eu.SSI.501	Req	The component shall assign the data point with ID sec.tls.cf to log level SEC_WARN.
Eu.SSI.502	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.cf.

ID	Type	Requirement
Eu.SSI.503	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.cf.
Eu.SSI.504	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cf.
Eu.SSI.505	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cf.
Eu.SSI.506	Req	The component shall add the transport layer error description using the parameter "errorMsg" with data type String to data point with ID sec.tls.cf.
Eu.SSI.507	Head	4.4.7.10 TLS Connection Attempt Failed due to Invalid Cipher: sec.tls.cfici
Eu.SSI.508	Req	If the component detects that a TLS connection attempt failed because no common cipher could be found, the component shall log the data point ID "sec.tls.cfici".
Eu.SSI.509	Req	The component shall assign the data point with ID sec.tls.cfici to log level SEC_WARN.
Eu.SSI.510	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.cfici.
Eu.SSI.511	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.cfici.
Eu.SSI.512	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cfici.
Eu.SSI.513	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cfici.
Eu.SSI.514	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter "certCN" with data type String to data point with ID sec.tls.cfici.
Eu.SSI.515	Head	4.4.7.11 TLS Connected: sec.tls.cuci
Eu.SSI.516	Info	Log data point deleted.
Eu.SSI.517	Head	4.4.7.12 TLS Connection Attempt Failed due to Wrong Key Exchange Method: sec.tls.cfwke
Eu.SSI.518	Req	If the component detects that a TLS connection attempt failed because the key exchange method did not match, the component shall log the data point ID "sec.tls.cfwke".
Eu.SSI.519	Req	The component shall assign the data point with ID sec.tls.cfwke to log level SEC_WARN.
Eu.SSI.520	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.cfwke.
Eu.SSI.521	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.cfwke.
Eu.SSI.522	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cfwke.
Eu.SSI.523	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cfwke.
Eu.SSI.524	Req	The component shall add the common name of the TLS certificate used by the connecting party using the parameter "certCN" with data type String to data point with ID sec.tls.cfwke.
Eu.SSI.525	Head	4.4.7.13 TLS Error of Underlying Library: sec.tls.emtls
Eu.SSI.526	Info	Log data point deleted.
Eu.SSI.527	Head	4.4.7.14 TLS Connect Request: sec.tls.cr
Eu.SSI.528	Req	If the component sends or receives a TLS connection request, the component shall log the data point ID "sec.tls.cr".
Eu.SSI.529	Req	The component shall assign the data point with ID sec.tls.cr to log level SEC_INFO.
Eu.SSI.530	Req	The component shall add the local IP address of the TLS connection using the parameter "locIP" with data type String to data point with ID sec.tls.cr.
Eu.SSI.531	Req	The component shall add the remote IP address of the TLS connection using the parameter "remoteIP" with data type String to data point with ID sec.tls.cr.
Eu.SSI.532	Req	The component shall add the local port of the TLS connection using the parameter "locPort" with data type UInt16 to data point with ID sec.tls.cr.
Eu.SSI.533	Req	The component shall add the remote port of the TLS connection using the parameter "remotePort" with data type UInt16 to data point with ID sec.tls.cr.
Eu.SSI.534	Req	The component shall add the common name of the TLS certificate used by the requesting party using the parameter "certCN" with data type String to data point with ID sec.tls.cr.

ID	Type	Requirement
Eu.SSI.535	Head	4.4.7.15 TLS Terminate Request: sec.tls.ct
Eu.SSI.536	Req	If the component sends or receives a TLS connection termination request, the component shall log the data point ID “sec.tls.ct”.
Eu.SSI.537	Req	The component shall assign the data point with ID sec.tls.ct to log level SEC_INFO.
Eu.SSI.538	Req	The component shall add the local IP address of the TLS connection using the parameter “locIP” with data type String to data point with ID sec.tls.ct.
Eu.SSI.539	Req	The component shall add the remote IP address of the TLS connection using the parameter “remoteIP” with data type String to data point with ID sec.tls.ct.
Eu.SSI.540	Req	The component shall add the local port of the TLS connection using the parameter “locPort” with data type UInt16 to data point with ID sec.tls.ct.
Eu.SSI.541	Req	The component shall add the remote port of the TLS connection using the parameter “remotePort” with data type UInt16 to data point with ID sec.tls.ct.
Eu.SSI.542	Req	The component shall add the common name of the TLS certificate used by the requesting party using the parameter “certCN” with data type String to data point with ID sec.tls.ct.
Eu.SSI.543	Head	4.4.8 Log requirements for Interlocking (EIL) (sec.eil.*)
Eu.SSI.544	Head	4.4.8.1 Misconfigured Connections Detected: sec.eil.miscon
Eu.SSI.545	Info	Log data point replaced by sec.pdi.miscon.
Eu.SSI.546	Head	4.4.8.2 Misconfigured Aystem Associations Detected: sec.eil.missys
Eu.SSI.547	Info	Log data point replaced by sec.pdi.missys.
Eu.SSI.548	Head	4.4.8.3 EfeS Unavailable: sec.eil.ccuv
Eu.SSI.549	Info	Log data point replaced by sec.pdi.timeout.
Eu.SSI.550	Head	4.4.8.4 EfeS Connection Timeout: sec.eil.occt
Eu.SSI.551	Info	Log data point replaced by sec.pdi.timeout.
Eu.SSI.552	Head	4.4.8.5 RBC Connection Timeout: sec.eil.rbcct
Eu.SSI.553	Info	Log data point replaced by sec.pdi.timeout.
Eu.SSI.554	Head	4.4.8.6 TCS Connection Timeout: sec.eil.tbcct
Eu.SSI.555	Info	Log data point replaced by sec.pdi.timeout.
Eu.SSI.556	Head	4.4.8.7 Failure of EfeS Area Detected: sec.eil.fare
Eu.SSI.557	Info	Log data point deleted.
Eu.SSI.558	Head	4.4.9 Log requirements for systems connected via SCI-XX.PDI (sec.pdi.*)
Eu.SSI.559	Head	4.4.9.1 Misconfigured Connections Detected: sec.pdi.miscon
Eu.SSI.560	Req	If the component detects a mismatch of communication parameters, the component shall log the data point ID “sec.pdi.miscon”.
Eu.SSI.561	Req	The component shall assign the data point with ID sec.pdi.miscon to log level SEC_ALERT.
Eu.SSI.562	Req	The component shall add the remote PDI identifier of the connection using the parameter “remoteId” with data type String to data point with ID sec.pdi.miscon.
Eu.SSI.563	Req	The component shall add the local PDI identifier of the connection using the parameter “locId” with data type String to data point with ID sec.pdi.miscon.
Eu.SSI.564	Req	The component shall add the error description using the parameter “errorMsg” with data type String to data point with ID sec.pdi.miscon.
Eu.SSI.565	Head	4.4.9.2 Misconfigured System Associations Detected: sec.pdi.missys
Eu.SSI.566	Req	If the components detects a mismatch of system associations, the component shall log the data point ID “sec.pdi.missys”.

ID	Type	Requirement
Eu.SSI.567	Req	The component shall assign the data point with ID sec.pdi.missys to log level SEC_ALERT.
Eu.SSI.568	Req	The component shall add the remote PDI identifier of the connection using the parameter "remoteId" with data type String to data point with ID sec.pdi.missys.
Eu.SSI.569	Req	The component shall add the local PDI identifier of the connection using the parameter "locId" with data type String to data point with ID sec.pdi.missys.
Eu.SSI.570	Req	The component shall add the error description using the parameter "errorMsg" with data type String to data point with ID sec.pdi.missys.
Eu.SSI.571	Head	4.4.9.3 Connection Timeout: sec.pdi.timeout
Eu.SSI.572	Req	If the components detects a PDI connection timeout, the component shall log the data point ID "sec.pdi.timeout".
Eu.SSI.573	Req	The component shall assign the data point with ID sec.pdi.timeout to log level SEC_WARN.
Eu.SSI.574	Req	The component shall add the remote PDI identifier of the connection using the parameter "remoteId" with data type String to data point with ID sec.pdi.timeout.
Eu.SSI.575	Req	The component shall add the local PDI identifier of the connection using the parameter "locId" with data type String to data point with ID sec.pdi.timeout.
Eu.SSI.576	Head	4.4.9.4 Packet not Treated due to Failed Identifier Check: sec.pdi.idchk
Eu.SSI.577	Req	If the component does not treat a packet due to a failed identifier check, the component shall log the data point ID "sec.pdi.idchk".
Eu.SSI.578	Req	The component shall assign the data point with ID sec.pdi.idchk to log level SEC_ALERT.
Eu.SSI.579	Req	The component shall add the remote PDI identifier of the connection using the parameter "remoteId" with data type String to data point with ID sec.pdi.idchk.
Eu.SSI.580	Req	The component shall add the local PDI identifier of the connection using the parameter "locId" with data type String to data point with ID sec.pdi.idchk.
Eu.SSI.581	Head	4.4.9.5 PDI Connection Closed: sec.pdi.closed
Eu.SSI.582	Req	If the component closes a PDI connection, the component shall log the data point ID "sec.pdi.closed".
Eu.SSI.583	Req	The component shall assign the data point with ID sec.pdi.closed to log level SEC_INFO.
Eu.SSI.584	Req	The component shall add the remote PDI identifier of the connection using the parameter "remoteId" with data type String to data point with ID sec.pdi.closed.
Eu.SSI.585	Req	The component shall add the local PDI identifier of the connection using the parameter "locId" with data type String to data point with ID sec.pdi.closed.
Eu.SSI.586	Head	4.4.10 Log Requirements for Components
Eu.SSI.587	Head	4.4.10.1 Connection to Device Established: sec.efes.cest
Eu.SSI.588	Info	Log data point deleted.
Eu.SSI.589	Head	4.4.10.2 Connection Attempt to Device Failed: sec.efes.cfai
Eu.SSI.590	Info	Log data point deleted.
Eu.SSI.591	Head	4.4.10.3 Connection Attempt to Device Rejected: sec.efes.crej
Eu.SSI.592	Info	Log data point deleted.
Eu.SSI.593	Head	4.4.10.4 Connection Attempt to Management Port: sec.efes.mgmt
Eu.SSI.594	Info	Log data point deleted.
Eu.SSI.595	Head	4.4.10.5 Disabled Port Activated / In Use: sec.efes.dprta
Eu.SSI.596	Info	Log data point deleted.
Eu.SSI.597	Head	4.4.10.6 Report on Activated Ports: sec.efes.rprt
Eu.SSI.598	Info	Log data point deleted.

ID	Type	Requirement
Eu.SSI.599	Head	4.4.10.7 Detected State Change Changing in Connections/Cabling: sec.efes.cbl
Eu.SSI.600	Info	Log data point deleted.
Eu.SSI.601	Head	4.4.10.8 Installation/Deployment of Software/Configarutions Started/Finished: sec.efes.depl
Eu.SSI.602	Info	Log data point deleted.
Eu.SSI.603	Head	4.4.10.9 Component Integrity Check Failed: sec.efes.intcf
Eu.SSI.604	Info	Log data point replaced by sec.comp.intcf
Eu.SSI.605	Head	4.4.10.10 Component Integrity Check Failed: sec.comp.intcf
Eu.SSI.606	Req	If a component detects that an integrity self-check failed, the component shall log the data point ID "sec.comp.intcf".
Eu.SSI.607	Req	The component shall assign the data point with ID sec.comp.intcf to log level SEC_ALERT.
Eu.SSI.608	Head	4.4.10.11 Component Integrity Check Successful: sec.efes.intcs
Eu.SSI.609	Info	Log data point replaced by sec.comp.intcs
Eu.SSI.610	Head	4.4.10.12 Component Integrity Check Successful: sec.comp.intcs
Eu.SSI.611	Req	If a component detects that an integrity self-check was successful, the component shall log the data point ID "sec.comp.intcs".
Eu.SSI.612	Req	The component shall assign the data point with ID sec.comp.intcs to log level SEC_INFO.
Eu.SSI.613	Head	4.4.10.13 Overheat Detected (in cabinet): sec.efes.heatc
Eu.SSI.614	Info	Log data point replaced by sec.comp.heatc
Eu.SSI.615	Head	4.4.10.14 Overheat Detected in Surrounding Environment: sec.comp.heatc
Eu.SSI.616	Req	If the component detects overheating in the surrounding environment, the component shall log the data point ID "sec.comp.heatc".
Eu.SSI.617	Req	The component shall assign the data point with ID sec.comp.heatc to log level SEC_WARN.
Eu.SSI.618	Req	The component shall add the temperature in degrees Celcius using the parameter "temp" with data type UInt8 to data point with ID sec.comp.heatc.
Eu.SSI.619	Head	4.4.10.15 Overheat Detected in Device: sec.efes.heatd
Eu.SSI.620	Info	Log data point replaced by sec.comp.heatd
Eu.SSI.621	Head	4.4.10.16 Overheat Detected in Component: sec.comp.heatd
Eu.SSI.622	Req	If the component detects internal overheating , the component shall log the data point ID "sec.comp.heatd".
Eu.SSI.623	Req	The component shall assign the data point with ID sec.comp.heatd to log level SEC_WARN.
Eu.SSI.624	Req	The component shall add the temperature in degrees Celcius using the parameter "temp" with data type UInt8 to data point with ID sec.comp.heatd.
Eu.SSI.625	Head	4.4.11 Log requirements for MDM
Eu.SSI.626	Head	4.4.11.1 Deployment Started: sec.mdm.depl
Eu.SSI.627	Info	Log data point replaced by sec.mdm.deplb and sec.mdm.deple.
Eu.SSI.628	Head	4.4.11.2 Deployment Started: sec.mdm.deplb
Eu.SSI.629	Req	If the MDM starts the deployment process for software or configuration, the MDM shall log the data point ID "sec.mdm.deplb".
Eu.SSI.630	Req	The MDM shall assign the data point with ID sec.mdm.deplb to log level SEC_INFO.

ID	Type	Requirement
Eu.SSI.631	Req	The MDM shall add the technical identifier (EULYNX) of the deployment target using the parameter "techID" with data type String to data point with ID sec.mdm.deplb.
Eu.SSI.632	Req	The MDM shall add the information which type of data is deployed using the parameter "dataType" and either the value "configuration" or "software" with data type String to data point with ID sec.mdm.deplb.
Eu.SSI.633	Head	4.4.11.3 Deployment Finished: sec.mdm.deple
Eu.SSI.634	Req	If the MDM finished the deployment process for software or configuration, the MDM shall log the data point ID "sec.mdm.deple".
Eu.SSI.635	Req	The MDM shall assign the data point with ID sec.mdm.deple to log level SEC_INFO.
Eu.SSI.636	Req	The MDM shall add the technical identifier (EULYNX) of the deployment target using the parameter "techID" with data type String to data point with ID sec.mdm.deple.
Eu.SSI.637	Req	The MDM shall add the information which type of data is deployed using the parameter "dataType" and either the value "configuration" or "software" with data type String to data point with ID sec.mdm.deplb.
Eu.SSI.638	Head	4.4.11.4 Integrity Check of Component Failed: sec.mdm.intcf
Eu.SSI.639	Req	If the MDM triggered an integrity check on a component which failed, the MDM shall log the data point ID "sec.mdm.intcf".
Eu.SSI.640	Req	The MDM shall assign the data point with ID sec.mdm.intcf to log level SEC_ALERT.
Eu.SSI.641	Req	The MDM shall add the technical identifier (EULYNX) of the integrity check target using the parameter "techID" with data type String to data point with ID sec.mdm.intcf.
Eu.SSI.642	Head	4.4.11.5 Integrity Check of Component Successful: sec.mdm.intcs
Eu.SSI.643	Req	If the MDM triggered an integrity check on a component which was successful, the MDM shall log the data point ID "sec.mdm.intcs".
Eu.SSI.644	Req	The MDM shall assign the data point with ID sec.mdm.intcs to log level SEC_INFO.
Eu.SSI.645	Req	The MDM shall add the technical identifier (EULYNX) of the integrity check target using the parameter "techID" with data type String to data point with ID sec.mdm.intcs.
Eu.SSI.646	Head	4.4.11.6 Device not Available: sec.mdm.unav
Eu.SSI.647	Req	If the MDM detects that a component was unexpectedly not connected for more than 1 day, the MDM shall log the data point ID "sec.mdm.unav".
Eu.SSI.648	Req	The MDM shall assign the data point with ID sec.mdm.unav to log level SEC_WARN.
Eu.SSI.649	Req	The MDM shall add the technical identifier (EULYNX) of unavailable component using the parameter "techID" with data type String to data point with ID sec.mdm.unav.
Eu.SSI.650	Head	4.4.11.7 Unkown Device: sec.mdm.devuk
Eu.SSI.651	Req	If the MDM receives a connection request from an unknown component, the MDM shall log the data point ID "sec.mdm.devuk".
Eu.SSI.652	Req	The component shall assign the data point with ID sec.mdm.devuk to log level SEC_ALERT.
Eu.SSI.653	Req	The MDM shall add the technical identifier (EULYNX) of unknown component using the parameter "techID" with data type String to data point with ID sec.mdm.devuk.
Eu.SSI.654	Head	4.4.11.8 Unknown Connection Identified: sec.mdm.conuk
Eu.SSI.655	Info	Log data point deleted.
Eu.SSI.656	Head	4.4.12 Log requirements for Backup Services
Eu.SSI.657	Head	4.4.12.1 Backup Started: sec.ssi.backup.started
Eu.SSI.658	Req	If the Backup Service starts the backup process of a client, the Backup Service shall log the data point ID "sec.ssi.backup.started".
Eu.SSI.659	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.started to log level SEC_INFO.
Eu.SSI.660	Req	The Backup Service shall add the IP address of the client using the parameter "peerIP" with data type String to data point with ID sec.ssi.backup.started.
Eu.SSI.661	Head	4.4.12.2 Backup Received: sec.ssi.backup.rec
Eu.SSI.662	Req	If the Backup Service completely received a backup, the Backup Service shall log the data point ID "sec.ssi.backup.rec".

ID	Type	Requirement
Eu.SSI.663	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.rec to log level SEC_INFO.
Eu.SSI.664	Req	The Backup Service shall add the IP address of the client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.rec.
Eu.SSI.665	Head	4.4.12.3 Backup Rejected due to Integrity Check Failure: sec.ssi.backup.rej
Eu.SSI.666	Req	If the Backup Service rejects a backup due to an backup file integrity check failure, the Backup Service shall log the data point ID “sec.ssi.backup.rej”.
Eu.SSI.667	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.rej to log level SEC_WARN.
Eu.SSI.668	Req	The Backup Service shall add the IP address of the client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.rej.
Eu.SSI.669	Head	4.4.12.4 Backup Requested: sec.ssi.backup.req
Eu.SSI.670	Info	Log data point deleted
Eu.SSI.671	Head	4.4.12.5 Restore Started: sec.ssi.backup.reststarted
Eu.SSI.672	Req	If a restore process is started by the Backup Service, the Backup Service shall log the data point ID “sec.ssi.backup.reststarted”.
Eu.SSI.673	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.reststarted to log level SEC_INFO.
Eu.SSI.674	Req	The Backup Service shall add the IP address of the client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.reststarted.
Eu.SSI.675	Req	The Backup Service shall add the timestamp of the restored backup using the parameter “bkpTs” with data type Timestamp to data point with ID sec.ssi.backup.reststarted.
Eu.SSI.676	Head	4.4.12.6 Restore Completed: sec.ssi.backup.restcomp
Eu.SSI.677	Req	If a restore process is completed by the Backup Service, the Backup Service shall log the data point ID “sec.ssi.backup.restcomp”.
Eu.SSI.678	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.restcomp to log level SEC_INFO.
Eu.SSI.679	Req	The Backup Service shall add the IP address of the client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.restcomp.
Eu.SSI.680	Req	The Backup Service shall add the timestamp of the restored backup using the parameter “bkpTs” with data type Timestamp to data point with ID sec.ssi.backup.restcomp.
Eu.SSI.681	Head	4.4.12.7 Backup Request Rejected: sec.ssi.backup.reqf
Eu.SSI.682	Info	Log data point deleted
Eu.SSI.683	Head	4.4.12.8 Backup Connection Rejected: sec.ssi.backup.crej
Eu.SSI.684	Req	If the Backup Service rejects a connection by client, the Backup Service shall log the data point ID “sec.ssi.backup.crej”.
Eu.SSI.685	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.crej to log level SEC_WARN.
Eu.SSI.686	Req	The Backup Service shall add the IP address of the client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.crej.
Eu.SSI.687	Head	4.4.12.9 Backup Authorisation Failed: sec.ssi.backup.af
Eu.SSI.688	Req	If the Backup Service rejects a backup or backup restore process due to missing authorisation of the client, the Backup Service shall log the data point ID “sec.ssi.backup.af”.
Eu.SSI.689	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.af to log level SEC_WARN.
Eu.SSI.690	Req	The Backup Service shall add the IP address of the client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.af.
Eu.SSI.691	Head	4.4.12.10 Missing Backup Detected: sec.ssi.backup.miss
Eu.SSI.692	Req	If the Backup Service detects that a backup is missing, the Backup Service shall log the data point ID “sec.ssi.backup.miss”.
Eu.SSI.693	Req	The component shall assign the data point with ID sec.ssi.backup.miss to log level SEC_WARN.
Eu.SSI.694	Req	The Backup Service shall add the IP address of the affected client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.miss.

ID	Type	Requirement
Eu.SSI.695	Req	The Backup Service shall add the timestamp of the affected backup using the parameter “bkpTs” with data type Timestamp to data point with ID sec.ssi.backup.miss.
Eu.SSI.696	Head	4.4.12.11 Corrupted or Damaged Backup Detected: sec.ssi.backup.dmg
Eu.SSI.697	Req	If the Backup Service detects a corrupted or damaged backup, the Backup Service shall log the data point ID “sec.ssi.backup.dmg”.
Eu.SSI.698	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.dmg to log level SEC_WARN.
Eu.SSI.699	Req	The Backup Service shall add the IP address of the affected client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.dmg.
Eu.SSI.700	Req	The Backup Service shall add the timestamp of the affected backup using the parameter “bkpTs” with data type Timestamp to data point with ID sec.ssi.backup.dmg.
Eu.SSI.701	Head	4.4.12.12 Error Saving Backup: sec.ssi.backup.svgerr
Eu.SSI.702	Info	Log data point deleted
Eu.SSI.703	Head	4.4.12.13 Error in Backup Connection: sec.ssi.backup.conerr
Eu.SSI.704	Req	If the Backup Service detects an error in a connection to a client, the Backup Service shall log the data point ID “sec.ssi.backup.conerr”.
Eu.SSI.705	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.conerr to log level SEC_WARN.
Eu.SSI.706	Req	The Backup Service shall add the IP address of the affected client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.conerr.
Eu.SSI.707	Head	4.4.12.14 Connection Aborted by Client: sec.ssi.backup.conabo
Eu.SSI.708	Req	If the Backup Service detects that a connection to a client is aborted by the client, the component shall log the data point ID “sec.ssi.backup.conabo”.
Eu.SSI.709	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.conabo to log level SEC_WARN.
Eu.SSI.710	Req	The Backup Service shall add the IP address of the affected client using the parameter “peerIP” with data type String to data point with ID sec.ssi.backup.conabo.
Eu.SSI.711	Head	4.4.12.15 Internal Error: sec.ssi.backup.interr
Eu.SSI.712	Req	If the Backup Service detects an internal error and if this case is not covered by other Backup Service log data points, the component shall log the data point ID “sec.ssi.backup.interr”.
Eu.SSI.713	Req	The Backup Service shall assign the data point with ID sec.ssi.backup.interr to log level SEC_WARN.
Eu.SSI.714	Req	The Backup Service shall add the error message using the parameter “errorMsg” with data type String to data point with ID sec.ssi.backup.interr.
Eu.SSI.715	Head	4.4.13 Log requirements for Time Services
Eu.SSI.716	Head	4.4.13.1 Failed Time Synchronisation: sec.ssi.time.fts
Eu.SSI.717	Req	If the component fails to perform time synchronisation, the component shall log the data point ID “sec.ssi.time.fts”.
Eu.SSI.718	Req	The component shall assign the data point with ID sec.ssi.time.fts to log level SEC_WARN.
Eu.SSI.719	Req	The component shall add the IP address of the time server using the parameter “serverIP” with data type String to data point with ID sec.ssi.time.fts.
Eu.SSI.720	Head	4.4.13.2 Failed Time Synchronisation with Details: sec.ssi.time.ftsd
Eu.SSI.721	Info	Log data point deleted
Eu.SSI.722	Head	4.4.13.3 Time Synchronisation Successful: sec.ssi.time.sts
Eu.SSI.723	Req	If the component sucessfully completed time synchronisation, the component shall log the data point ID “sec.ssi.time.sts”.
Eu.SSI.724	Req	The component shall assign the data point with ID sec.ssi.time.sts to log level SEC_INFO.
Eu.SSI.725	Head	4.4.13.4 Time Synchronization Successful with Details: sec.ssi.time.stsd
Eu.SSI.726	Info	Log data point deleted

ID	Type	Requirement
Eu.SSI.727	Head	4.4.14 Log requirements for Certificate Process
Eu.SSI.728	Head	4.4.14.1 New Certificate Used: sec.ssi.cert.unc
Eu.SSI.729	Req	If the component is using a certificate for the first time, the component shall log the data point ID "sec.ssi.cert.unc".
Eu.SSI.730	Req	The component shall assign the data point with ID sec.ssi.cert.unc to log level SEC_INFO.
Eu.SSI.731	Req	The component shall add the common name of the certificate using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.unc.
Eu.SSI.732	Req	The component shall add the serial number of the certificate using the parameter "certSN" with data type String to data point with ID sec.ssi.cert.unc.
Eu.SSI.733	Head	4.4.14.2 New Certificate used by EIL: sec.ssi.cert.eil.unc
Eu.SSI.734	Info	Log data point replaced by sec.ssi.cert.unc.
Eu.SSI.735	Head	4.4.14.3 New Certificate used by EfeS: sec.ssi.cert.efes.unc
Eu.SSI.736	Info	Log data point replaced by sec.ssi.cert.unc.
Eu.SSI.737	Head	4.4.14.4 New Certificate used by MDM: sec.ssi.cert.mdm.unc
Eu.SSI.738	Info	Log data point replaced by sec.ssi.cert.unc.
Eu.SSI.739	Head	4.4.14.5 Renewal of Certificate: sec.ssi.cert.rnc
Eu.SSI.740	Req	If the component received a renewed certificate, the component shall log the data point ID "sec.ssi.cert.rnc".
Eu.SSI.741	Req	The component shall assign the data point with ID sec.ssi.cert.rnc to log level SEC_INFO.
Eu.SSI.742	Req	The component shall add the common name of the certificate using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.rnc.
Eu.SSI.743	Req	The component shall add the serial number of the certificate using the parameter "certSN" with data type String to data point with ID sec.ssi.cert.rnc.
Eu.SSI.744	Head	4.4.14.6 Renewal of Certificate for EIL: sec.ssi.cert.eil.rnc
Eu.SSI.745	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.746	Head	4.4.14.7 Renewal of Certificate for EfeS: sec.ssi.cert.efes.rnc
Eu.SSI.747	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.748	Head	4.4.14.8 Renewal of Certificate for MDM: sec.ssi.cert.mdm.rnc
Eu.SSI.749	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.750	Head	4.4.14.9 Sending Signing Request for a Certificate: sec.ssi.cert.rec
Eu.SSI.751	Req	If the component is sending a certificate signing request, the component shall log the data point ID "sec.ssi.cert.rec".
Eu.SSI.752	Req	The component shall assign the data point with ID sec.ssi.cert.rec to log level SEC_INFO.
Eu.SSI.753	Req	The component shall add the common name included in the certificate signing request using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.rec.
Eu.SSI.754	Head	4.4.14.10 Sending Signing Request of a Certificate for EIL: sec.ssi.cert.eil.rec
Eu.SSI.755	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.756	Head	4.4.14.11 Sending Signing Request of a Certificate for EfeS: sec.ssi.cert.efes.rec
Eu.SSI.757	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.758	Head	4.4.14.12 Sending Signing Request of a Certificate for MDM: sec.ssi.cert.mdm.rec

ID	Type	Requirement
Eu.SSI.759	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.760	Head	4.4.14.13 Update of CRL: sec.ssi.cert.ucrl
Eu.SSI.761	Req	If the component fetched an CRL, the component shall log the data point ID "sec.ssi.cert.ucrl".
Eu.SSI.762	Req	The component shall assign the data point with ID sec.ssi.cert.ucrl to log level SEC_INFO.
Eu.SSI.763	Req	The component shall add the distribution point of the CRL using the parameter "distributionPoint" with data type String to data point with ID sec.ssi.cert.ucrl.
Eu.SSI.764	Req	The component shall add the issuing timestamp of the CRL using the parameter "issuedAt" with data type Timestamp to data point with ID sec.ssi.cert.ucrl.
Eu.SSI.765	Head	4.4.14.14 Update of CRL for EIL: sec.ssi.cert.eil.ucrl
Eu.SSI.766	Info	Log data point replaced by sec.ssi.cert.ucrl.
Eu.SSI.767	Head	4.4.14.15 Update of CRL for EfeS: sec.ssi.cert.eil.ucrl
Eu.SSI.768	Info	Log data point replaced by sec.ssi.cert.ucrl.
Eu.SSI.769	Head	4.4.14.16 Update of CRL for MDM: sec.ssi.cert.eil.ucrl
Eu.SSI.770	Info	Log data point replaced by sec.ssi.cert.ucrl.
Eu.SSI.771	Head	4.4.14.17 Issued New Certificate: sec.ssi.cert.inc
Eu.SSI.772	Req	If the PKI issued a certificate, the PKI shall log the data point ID "sec.ssi.cert.inc".
Eu.SSI.773	Req	The PKI shall assign the data point with ID sec.ssi.cert.inc to log level SEC_INFO.
Eu.SSI.774	Req	The PKI shall add the common name included in the certificate signing request using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.inc.
Eu.SSI.775	Req	The PKI shall add the serial number of the certificate using the parameter "certSN" with data type String to data point with ID sec.ssi.cert.inc.
Eu.SSI.776	Head	4.4.14.18 Receiving Signing Request for a Certificate: sec.ssi.cert.rnc
Eu.SSI.777	Req	If the PKI received a certificate signing request, the PKI shall log the data point ID "sec.ssi.cert.rnc".
Eu.SSI.778	Req	The PKI shall assign the data point with ID sec.ssi.cert.rnc to log level SEC_INFO.
Eu.SSI.779	Req	The PKI shall add the common name included in the certificate signing request using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.rnc.
Eu.SSI.780	Head	4.4.14.19 Receiving Signing Request for a Certificate by PKI RA: sec.ssi.cert.pki_ra.rnc
Eu.SSI.781	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.782	Head	4.4.14.20 Receiving Signing Request for a Certificate by PKI CA: sec.ssi.cert.pki_ca.rnc
Eu.SSI.783	Info	Log data point replaced by sec.ssi.cert.rnc.
Eu.SSI.784	Head	4.4.14.21 Revocation of Certificate: sec.ssi.cert.rec
Eu.SSI.785	Req	If the PKI revoked a certificate, the PKI shall log the data point ID "sec.ssi.cert.rec".
Eu.SSI.786	Req	The PKI shall assign the data point with ID sec.ssi.cert.rec to log level SEC_INFO.
Eu.SSI.787	Req	The PKI shall add the common name of the revoked certificate using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.rec.
Eu.SSI.788	Req	The PKI shall add the serial number of the revoked certificate using the parameter "certSN" with data type String to data point with ID sec.ssi.cert.rec.
Eu.SSI.789	Head	4.4.14.22 Revocation of Certificate: sec.ssi.cert.pki_ca.rec
Eu.SSI.790	Info	Log data point replaced by sec.ssi.cert.rec.

ID	Type	Requirement
Eu.SSI.791	Head	4.4.14.23 Failed Validation of Certificate: sec.ssi.cert.fvc
Eu.SSI.792	Req	If the component fails to validate a certificate, the component shall log the data point ID "sec.ssi.cert.fvc".
Eu.SSI.793	Req	The component shall assign the data point with ID sec.ssi.cert.fvc to log level SEC_WARN.
Eu.SSI.794	Req	The component shall add the common name of the certificate using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.fvc.
Eu.SSI.795	Req	The component shall add the serial number of the certificate using the parameter "certSN" with data type String to data point with ID sec.ssi.cert.fvc.
Eu.SSI.796	Head	4.4.14.24 Failed Validation of Certificate for EIL: sec.ssi.cert.eil.fvc
Eu.SSI.797	Info	Log data point replaced by sec.ssi.cert.fvc.
Eu.SSI.798	Head	4.4.14.25 Failed Validation of Certificate for EfeS: sec.ssi.cert.efes.fvc
Eu.SSI.799	Info	Log data point replaced by sec.ssi.cert.fvc.
Eu.SSI.800	Head	4.4.14.26 Failed Validation of Certificate for MDM: sec.ssi.cert.mdm.fvc
Eu.SSI.801	Info	Log data point replaced by sec.ssi.cert.fvc.
Eu.SSI.802	Head	4.4.14.27 Successful Validation of Certificate: sec.ssi.cert.pvc
Eu.SSI.803	Req	If the component successfully validated a certificate, the component shall log the data point ID "sec.ssi.cert.pvc".
Eu.SSI.804	Req	The component shall assign the data point with ID sec.ssi.cert.pvc to log level SEC_INFO.
Eu.SSI.805	Req	The component shall add the common name of the certificate using the parameter "certCN" with data type String to data point with ID sec.ssi.cert.pvc.
Eu.SSI.806	Req	The component shall add the serial number of the certificate using the parameter "certSN" with data type String to data point with ID sec.ssi.cert.pvc.
Eu.SSI.807	Head	4.4.14.28 Successful Validation of Certificate for EIL: sec.ssi.cert.eil.pvc
Eu.SSI.808	Info	Log data point replaced by sec.ssi.cert.pvc.
Eu.SSI.809	Head	4.4.14.29 Successful Validation of Certificate for EfeS: sec.ssi.cert.efes.pvc
Eu.SSI.810	Info	Log data point replaced by sec.ssi.cert.pvc.
Eu.SSI.811	Head	4.4.14.30 Successful Validation of Certificate for MDM: sec.ssi.cert.mdm.pvc
Eu.SSI.812	Info	Log data point replaced by sec.ssi.cert.pvc.
Eu.SSI.813	Head	4.4.14.31 Failed Access to Validation Endpoint: sec.ssi.cert.facrl
Eu.SSI.814	Req	If the component fails to access the validation endpoint, the component shall log the data point ID "sec.ssi.cert.facrl".
Eu.SSI.815	Req	The component shall assign the data point with ID sec.ssi.cert.facrl to log level SEC_WARN.
Eu.SSI.816	Req	The component shall add the address of the failing validation endpoint using the parameter "endPoint" with data type String to data point with ID sec.ssi.cert.facrl.
Eu.SSI.817	Head	4.4.14.32 Failed Access to Validation Service for EIL: sec.ssi.cert.eil.facrl
Eu.SSI.818	Info	Log data point replaced by sec.ssi.cert.facrl.
Eu.SSI.819	Head	4.4.14.33 Failed Access to Validation Service for EfeS: sec.ssi.cert.efes.facrl
Eu.SSI.820	Info	Log data point replaced by sec.ssi.cert.facrl.
Eu.SSI.821	Head	4.4.14.34 Failed Access to Validation Service for MDM: sec.ssi.cert.mdm.facrl
Eu.SSI.822	Info	Log data point replaced by sec.ssi.cert.facrl.

ID	Type	Requirement
Eu.SSI.823	Head	4.4.15 Log requirements for Identity and Access Management
Eu.SSI.824	Info	Log data points sec.ssi.iam.* deleted.