www.streamx.ch

IEC 62351-5
Security conformance for:

StreamBridge: Stream870-5-104

Controlling station definition (Master)

September 02, 2021

Version Informations

Historic			
Date	Author	Description	Version
04/12/2021	Elvexys / FD	Initial version	0.01
05/11/2021	Elvexys / FD	Statistic information	1.00
09/02/2021	Elvexys / FD	Add symmetric update key change method	1.01

Version audit			
Date	Auditor	File	Version

Table of Contents

10. Protocol implementation conformance statement

10.1 Overview of clause

Implementors of this specification shall supply the information in Clause 11 on request. An “X” in a box means that the implementation supports the listed feature.

10.2 Required algorithms

If the implementor does not declare support for an algorithm marked “(required)”, interoperability cannot be guaranteed.

If an algorithm is not supported due to export restrictions, the implementor shall provide a copy of the export restriction that prohibits its export. This algorithm shall not be supported if and only if export restrictions do not allow any mechanism of exportation. If this algorithm is not supported, the implementation shall be clearly documented as adhering to the export restrictions, as supplied. The documentation shall also specify that the interoperable/base specification requirements are not supported. Samples of the documentation shall be provided.

10.3 MAC algorithms

- [X] HMAC-SHA-256 (required)
- [ ] Other _____

10.4 Key wrap algorithms

- [X] AES-256 Key Wrap (required)
- [ ] Other _____

10.5 Maximum Error messages sent

- [ ] Fixed at 2
- [X] Configurable

10.6 Use of Error messages

- [X] Transmits Error messages

10.7 Update Key Change Methods

- [X] None permitted
- [X] <4> Symmetric AES-256 / HMACSHA-256 (required)
- [ ] <5> Symmetric AES-256 / AES-GMAC
- [ ] <68> Asymmetric RSA-2048 / DSA SHA-256 (L=2048 N=256) / HMAC-SHA-256
- [ ] <69> Asymmetric RSA-3072 / DSA SHA-256 (L=3072 N=256) / AES-SHA-256
- [ ] <70> Asymmetric RSA-2048 / DSA SHA-256 (L=2048 N=256) / HMAC-GMAC
- [ ] <71> Asymmetric RSA-3072 / DSA SHA-256 (L=3072 N=256) / AES-GMAC
- [ ] Other _____

10.8 User Status Change

- [X] Non-certificate method (required)
- [ ] Use IEC/TS 62351-8 Certificates

10.9 Configurable parameters

Parameter	Configured at station	Value
Reply Timeout (sec)	Both	Configurable
Maximum Error Messages Sent	Both	Configurable
Session Key Change Interval (sec)	Controlling	Configurable
Session Key Change Count	Controlling	Configurable
Expected Session Key Change Interval (sec)	Controlled	Configurable
Expected Session Key Change Count	Controlled	Configurable
Maximum Session Key Status Count	Controlled	Configurable
Update Key Change Method	Both	Configurable
Authentication Challenge Data Length	Both	Configurable
Key Status Challenge Data Length	Controlled	Configurable
Controlling Station Challenge Data Length	Controlling	Configurable
Controlled Station Challenge Data Length	Controlled	Configurable
Maximum Certificate Size	Both	N/A
Maximum Number of Users	Both	1
Update Key(s)*	Both, if Update Key Change Method is “None permitted”.	Configurable
User Number(s)	Both, if Update Key Change Method is “None permitted”.	Configurable
User Name(s)	Controlling station or at the Authority, if Update Key change is permitted.	Configurable
Outstation Name(s)	Both, if Update Key change is permitted	Configurable
Authority Public Key* or Authority Certification Key*	Both, if Update Key change is permitted	Configurable
User Public Key(s)*	Controlling station or at the Authority	N/A
Outstation Public Key*	Controlling	N/A
* It is permitted to provide information about how to read or change the configured keys rather than entering the actual values of the keys in the PICS.		

10.10 Configurable statistic thresholds and statistic information object addresses

Name	Default value of statistic threshold (per IEC/TS 62351-5)	Configured value of statistic threshold	Information object address of the integrated total for the statistic
Unexpected Messages	3	3	Configurable
Authorization Failures	5	5	Configurable
Authentication Failures	5	5	Configurable
Reply Timeouts	3	3	Configurable
Rekeys Due to Authentication Failure	3	3	Configurable
Total Messages Sent	100	100	Configurable
Total Messages Received	100	100	Configurable
Critical Messages Sent	100	100	Configurable
Critical Messages Received	100	100	Configurable
Discarded Messages	10	10	Configurable
Error Messages Sent	10	10	Configurable
Error Messages Rxed	10	10	Configurable
Successful Authentications	100	100	Configurable
Session Key Changes	10	10	Configurable
Failed Session Key Changes	5	5	Configurable
Update Key Changes	1	1	Configurable
Failed Update Key Changes	1	1	Configurable
Rekeys Due to Restarts	3	3	Configurable

10.11 Critical functions

Complete this table to show which functions are considered critical by the device as it is presently configured. An “M” in the “M/O” column means it is mandatory to consider this Type to be critical. An “O” means it is optional. A “-“ in the “Configured as Critical” column means the type is not supported.

Type identification		Description	M/O	Configured as critical (Y/N/-)
<1>	M_SP_NA_1	Single-point information without time tag	O	N (Configurable)
<3>	M_DP_NA_1	Double-point information without time tag	O	N (Configurable)
<5>	M_ST_NA_1	Step position information	O	N (Configurable)
<7>	M_BO_NA_1	Bitstring of 32 bits	O	N (Configurable)
<9>	M_ME_NA_1	Measured value, normalized value	O	N (Configurable)
<11>	M_ME_NB_1	Measured value, scaled value	O	N (Configurable)
<13>	M_ME_NC_1	Measured value, short floating point number	O	N (Configurable)
<15>	M_IT_NA_1	Integrated totals	O	N (Configurable)
<20>	M_PS_NA_1	Packed single-point information with status	O	-
<21>	M_ME_ND_1	Measured value, normalized value without quality	O	-
<30>	M_SP_TB_1	Single-point information with time tag CP56Time2a	O	N (Configurable)
<31>	M_DP_TB_1	Double-point information with time tag CP56Time2a	O	N (Configurable)
<32>	M_ST_TB_1	Step position information with time tag CP56Time2a	O	N (Configurable)
<33>	M_BO_TB_1	Bitstring of 32 bits with time tag CP56Time2a	O	N (Configurable)
<34>	M_ME_TD_1	Measured value, normalized value with time tag CP56Time2a	O	N (Configurable)
<35>	M_ME_TE_1	Measured value, scaled value with time tag CP56Time2a	O	N (Configurable)
<36>	M_ME_TF_1	Measured value, short floating point number with time tag CP56Time2a	O	N (Configurable)
<37>	M_IT_TB_1	Integrated totals with time tag CP56Time2a	O	N (Configurable)
<38>	M_EP_TD_1	Event of protection equipment with time tag CP56Time2a	O	N (Configurable)
<39>	M_EP_TE_1	Packed start events of protection equipment with time tag CP56Time2a	O	N (Configurable)
<40>	M_EP_TF_1	Packed output circuit information of protection equipment with	O	N (Configurable)

		time tag CP56Time2a		
<45>	C_SC_NA_1	Single command	M	Y
<46>	C_DC_NA_1	Double command	M	Y
<47>	C_RC_NA_1	Regulating step command	M	Y
<48>	C_SE_NA_1	Set-point command, normalized value	M	Y
<49>	C_SE_NB_1	Set-point command, scaled value	M	Y
<50>	C_SE_NC_1	Set-point command, short floating-point number	M	Y
<51>	C_BO_NA_1	Bitstring of 32-bit	M	Y
<58>	C_SC_TA_1	Single command with time tag CP56Time2a	M	Y
<59>	C_DC_TA_1	Double command with time tag CP56Time2a	M	Y
<60>	C_RC_TA_1	Regulating step command with time tag CP56Time2a	M	Y
<61>	C_SE_TA_1	Set point command, normalized value with time tag CP56Time2a	M	Y
<62>	C_SE_TB_1	Set point command, scaled value with time tag CP56Time2a	M	Y
<63>	C_SE_TC_1	Set point command, short floating-point number with time tag CP56Time2a	M	Y
<64>	C_BO_TA_1	Bitstring of 32 bits with time tag CP56Time2a	M	Y
<70>	M_EI_NA_1	End of initialization	O	N (Configurable)
<100>	C_IC_NA_1	Interrogation command	O	N (Configurable)
<101>	C_CI_NA_1	Counter interrogation command	O	N (Configurable)
<102>	C_RD_NA_1	Read command	O	-
<103>	C_CS_NA_1	Clock synchronization command	M	Y
<105>	C_RP_NA_1	Reset process command	M	-
<107>	C_TS_TA_1	Test command with time tag CP56Time2a	O	N (Configurable)
<110>	P_ME_NA_1	Parameter of measured value, normalized value	M	-
<111>	P_ME_NB_1	Parameter of measured value, scaled value	M	-
<112>	P_ME_NC_1	Parameter of measured value, short floating-point number	M	-
<113>	P_AC_NA_1	Parameter activation	M	-
<120>	F_FR_NA_1	File ready	M	Y
<121>	F_SR_NA_1	Section ready	M	Y
<122>	F_SC_NA_1	Call directory, select file, call file, call section	M	Y
<123>	F_LS_NA_1	Last section, last segment	M	Y
<124>	F_AF_NA_1	Ack file, ack section	M	Y
<125>	F_SG_NA_1	Segment	M	Y
<126>	F_DR_TA_1	Directory	M	Y