



**Assurance Activity Report  
for  
KlasOS Keel Version 5.4.0**

KlasOS Keel 5.4.0 Security Target  
Version 1.5

**Collaborative Protection Profile for Network Devices Version 2.2e  
and  
PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e**

AAR Version 1.5, 16 July 2024

**Evaluated by:**



2400 Research Blvd, Suite 395  
Rockville, MD 20850

**Prepared for:**



**National Information Assurance Partnership  
Common Criteria Evaluation and Validation Scheme**

**The Developer of the TOE:**  
**Klas**

**The Author of the Security Target:**  
**Acumen Security, LLC.**

**The TOE Evaluation was Sponsored by:**  
**Klas**

**Evaluation Personnel:**  
Furukh Siddique  
Minal Wankhede  
Alexander Fannin  
Snehal Raghunath Gaonkar

**Common Criteria Version**  
Common Criteria Version 3.1 Revision 5

**Common Evaluation Methodology Version**  
CEM Version 3.1 Revision 5

## Revision History

VERSION	DATE	CHANGES
1.0	04/18/2024	Initial Release
1.1	04/24/2024	Updated to address lead review comments
1.2	05/10/2024	Updated based on internal reviews
1.3	05/21/2024	Updated based on Peer Lead Review comments
1.4	06/17/2024	Finalized AAR after QA review
1.5	07/16/2024	Updated to address ECR comments

## Contents

<b>1</b>	<b>TOE Overview .....</b>	<b>12</b>
1.1	TOE Description .....	12
1.1.1	Physical Boundaries .....	15
<b>2</b>	<b>Assurance Activities Identification .....</b>	<b>16</b>
<b>3</b>	<b>Test Equivalency Justification .....</b>	<b>17</b>
3.1	Architectural Description .....	17
3.1.1	Klas TRXr2.....	17
3.1.2	Klas Voyager VMm .....	17
3.1.3	Klas Voyager VM3 .....	17
3.2	Specification of Differences .....	17
3.3	Equivalency Analysis .....	19
3.3.1	Platform/Hardware Dependencies .....	19
3.3.2	Differences in Libraries Used to Provide TOE Functionality .....	19
3.3.3	TOE Management Interface Differences .....	19
3.3.4	TOE Functional Differences.....	20
3.3.5	Difference Comparison based on CPU micro-architecture.....	21
3.3.6	Klas Keel OS 5.4.0.....	21
3.3.7	Difference Comparison based on CPU Security features. ....	22
3.4	Recommendations/Conclusions.....	22
3.5	References .....	23
3.6	Appendix: Processor Technical Comparison .....	23
3.6.1	Klas TRXr2.....	23
3.6.2	Klas Voyager VMm .....	25
3.6.3	Klas Voyager VM3 .....	28
<b>4</b>	<b>Test Bed Descriptions .....</b>	<b>31</b>
4.1	Test Bed.....	31
4.1.1	Audit.....	31
4.1.2	Auth/Crypto/TLSS/Update .....	32
4.1.3	DTLSC.....	33
4.1.4	DTLSS/X509-Rev .....	34
4.1.5	DTLSS-MA .....	35
4.1.6	Firewall.....	36
4.1.7	SSHC .....	37
4.1.8	SSHS.....	38
4.2	Configuration Information .....	39
4.2.1	Audit.....	39
4.2.2	Auth/Crypto/TLSS/Update .....	39
4.2.3	DTLSC.....	40
4.2.4	DTLSS/X509-Rev .....	40

4.2.5	DTLSS-MA.....	41
4.2.6	Firewall.....	41
4.2.7	SSHC .....	42
4.2.8	SSHS.....	42
<b>4.3</b>	<b>Test Time and Location .....</b>	<b>42</b>
<b>5</b>	<b>Detailed Test Cases (TSS and the AGD Activities)</b> .....	<b>44</b>
<b>5.1</b>	<b>Mandatory Requirements .....</b>	<b>44</b>
5.1.1	Security Audit (FAU).....	44
5.1.2	Cryptographic Support (FCS).....	49
5.1.3	Identification and Authentication (FIA) .....	60
5.1.4	Security Management (FMT) .....	66
5.1.5	Protection of Security Functions (FPT) .....	71
5.1.6	TOE Access (FTA).....	79
5.1.7	Trusted Path (FTP).....	83
5.1.8	User Data Protection (FDP).....	87
5.1.9	Firewall (FFW) .....	87
5.1.10	Security management (FMT) .....	103
<b>5.2</b>	<b>Optional Requirements.....</b>	<b>104</b>
5.2.1	Security Audit (FAU).....	104
5.2.2	Cryptographic Support (FCS).....	105
<b>5.3</b>	<b>Selection-Based Requirements .....</b>	<b>110</b>
5.3.1	Cryptographic Support (FCS).....	110
5.3.2	Identification and Authentication (FIA) .....	137
5.3.3	Security Management (FMT) .....	141
<b>6</b>	<b>Security Assurance Requirements.....</b>	<b>147</b>
<b>6.1</b>	<b>TOE Summary Specification (ASE_TSS.1) .....</b>	<b>147</b>
6.1.1	ASE_TSS.1.1C.....	147
<b>6.2</b>	<b>Basic Functional Specification (ADV_FSP).....</b>	<b>147</b>
6.2.1	ADV_FSP.1.....	147
<b>6.3</b>	<b>Operational User Guidance (AGD_OPE) .....</b>	<b>148</b>
6.3.1	AGD_OPE.1.....	148
<b>6.4</b>	<b>Preparative Procedures (AGD_PRE) .....</b>	<b>151</b>
6.4.1	AGD_PRE.1 .....	151
<b>6.5</b>	<b>Assurance Activities (ALC).....</b>	<b>153</b>
6.5.1	ALC_CMC.1.....	153
6.5.2	ALC_CMS.1 .....	153
<b>6.6</b>	<b>Independent Testing – Conformance (ATE_IND) .....</b>	<b>154</b>
6.6.1	ATE_IND.1 .....	154
<b>6.7</b>	<b>Vulnerability Survey (AVA_VAN).....</b>	<b>154</b>
6.7.1	AVA_VAN.1.....	154

<b>7</b>	<b>Detailed Test Cases (Test Activities).....</b>	<b>157</b>
7.1	Auth.....	157
7.1.1	FAU_STG.1 Test #1 .....	157
7.1.2	FAU_STG.1 Test #2 .....	157
7.1.3	FIA_AFL.1 Test #1 .....	158
7.1.4	FIA_AFL.1 Test #2a .....	158
7.1.5	FIA_AFL.1 Test #2b .....	159
7.1.6	FIA_PMG_EXT.1 Test #1 .....	159
7.1.7	FIA_PMG_EXT.1 Test #2 .....	160
7.1.8	FIA_UIA_EXT.1 Test #1 .....	160
7.1.9	FIA_UIA_EXT.1 Test #2 .....	161
7.1.10	FIA_UIA_EXT.1 Test #3 .....	162
7.1.11	FIA_UIA_EXT.1 Test #4 .....	162
7.1.12	FIA_UAU.7 Test #1.....	162
7.1.13	FMT_MOF.1/AutoUpdate Test #1 .....	163
7.1.14	FMT_MOF.1/AutoUpdate Test #2 .....	163
7.1.15	FMT_MOF.1/ManualUpdate Test #1.....	163
7.1.16	FMT_MOF.1/ManualUpdate Test #2.....	164
7.1.17	FMT_MOF.1/Functions (1) Test #1 .....	164
7.1.18	FMT_MOF.1/Functions (1)Test #2 .....	165
7.1.19	FMT_MOF.1/Functions (2) Test #1 .....	166
7.1.20	FMT_MOF.1/Functions (2) Test #2 .....	166
7.1.21	FMT_MOF.1/Functions (3) Test #1 .....	166
7.1.22	FMT_MOF.1/Functions (3) Test #2 .....	167
7.1.23	FMT_MOF.1/Functions Test #3.....	167
7.1.24	FMT_MOF.1/Functions Test #4.....	167
7.1.25	FMT_MOF.1/Services Test #1 .....	168
7.1.26	FMT_MOF.1/Services Test #2 .....	168
7.1.27	FMT_MTD.1/CryptoKeys Test #1 .....	169
7.1.28	FMT_MTD.1/CryptoKeys Test #2 .....	169
7.1.29	FMT_SMF.1 Test #1 .....	170
7.1.30	FMT_SMR.2 Test #1.....	171
7.1.31	FTA_SSL.3 Test #1 .....	172
7.1.32	FTA_SSL.4 Test #1 .....	173
7.1.33	FTA_SSL.4 Test #2 .....	173
7.1.34	FTA_SSL_EXT.1.1 Test #1 .....	174
7.1.35	FTA_TAB.1 Test #1 .....	174
7.1.36	FTP_TRP.1/Admin Test #1.....	175
7.1.37	FTP_TRP.1/Admin Test #2.....	175
7.2	Audit.....	176
7.2.1	FAU_GEN.1 Test #1.....	176
7.2.2	FAU_GEN.1 Test #2.....	176

7.2.3	FAU_STG_EXT.1 Test #1	177
7.2.4	FAU_STG_EXT.1 Test #2 (a)	177
7.2.5	FAU_STG_EXT.1 Test #2 (b)	177
7.2.6	FAU_STG_EXT.1 Test #2 (c)	178
7.2.7	FAU_STG_EXT.1 Test #3	178
7.2.8	FAU_STG_EXT.1 Test #4	178
7.2.9	FAU_STG_EXT.2/LocSpace	179
7.2.10	FAU_STG_EXT.3/LocSpace Test#1	179
7.2.11	FAU_STG_EXT.3/LocSpace Test#2	179
7.2.12	FCS_NTP_EXT.1.1 Test #1	179
7.2.13	FCS_NTP_EXT.1.2 Test #1	180
7.2.14	FCS_NTP_EXT.1.3 Test #1	180
7.2.15	FCS_NTP_EXT.1.4 Test #1	181
7.2.16	FCS_NTP_EXT.1.4 Test #2	182
7.2.17	FPT_STM_EXT.1 Test #1	182
7.2.18	FPT_STM_EXT.1 Test #2	183
7.2.19	FPT_STM_EXT.1 Test #3	183
7.2.20	FTP_ITC.1 Test #1	183
7.2.21	FTP_ITC.1 Test #2	183
7.2.22	FTP_ITC.1 Test #3	184
7.2.23	FTP_ITC.1 Test #4	184
<b>7.3</b>	<b>Crypto</b>	<b>185</b>
7.3.1	FCS_CKM.1 RSA	185
7.3.2	FCS_CKM.1 ECC	185
7.3.3	FCS_CKM.1 FFC	186
7.3.4	FCS_CKM.2 SP800-56A	187
7.3.5	FCS_CKM.2 RSA	189
7.3.6	FCS_CKM.2 FFC	189
7.3.7	FCS_COP.1/DataEncryption AES-CBC KAT	189
7.3.8	FCS_COP.1/DataEncryption AES-CBC MBMT	191
7.3.9	FCS_COP.1/DataEncryption AES-CBC MCT	191
7.3.10	FCS_COP.1/DataEncryption AES-GCM	192
7.3.11	FCS_COP.1/SigGen ECDSA	193
7.3.12	FCS_COP.1/SigGen RSA	193
7.3.13	FCS_COP.1/Hash	194
7.3.14	FCS_COP.1/KeyedHash	195
7.3.15	FCS_RBG_EXT.1	195
<b>7.4</b>	<b>X509-Rev</b>	<b>196</b>
7.4.1	FIA_X509_EXT.1.1/Rev Test #1a	196
7.4.2	FIA_X509_EXT.1.1/Rev Test #1b	197
7.4.3	FIA_X509_EXT.1.1/Rev Test #2	197
7.4.4	FIA_X509_EXT.1.1/Rev Test #3	198

7.4.5	FIA_X509_EXT.1.1/Rev Test #4	199
7.4.6	FIA_X509_EXT.1.1/Rev Test #5	200
7.4.7	FIA_X509_EXT.1.1/Rev Test #6	201
7.4.8	FIA_X509_EXT.1.1/Rev Test #7	202
7.4.9	FIA_X509_EXT.1.1/Rev Test #8a	202
7.4.10	FIA_X509_EXT.1.1/Rev Test #8b	203
7.4.11	FIA_X509_EXT.1.1/Rev Test #8c	203
7.4.12	FIA_X509_EXT.1.2/Rev Test #1	204
7.4.13	FIA_X509_EXT.1.2/Rev Test #2	205
7.4.14	FIA_X509_EXT.2 Test #1	206
7.4.15	FIA_X509_EXT.3 Test #1	206
7.4.16	FIA_X509_EXT.3 Test #2	207
<b>7.5</b>	<b>DTLSS</b>	<b>207</b>
7.5.1	FCS_DTLSS_EXT.1.1 Test #1	207
7.5.2	FCS_DTLSS_EXT.1.1 Test #2	208
7.5.3	FCS_DTLSS_EXT.1.1 Test #3a	209
7.5.4	FCS_DTLSS_EXT.1.1 Test #3b	210
7.5.5	FCS_DTLSS_EXT.1.3 Test #1	211
7.5.6	FCS_DTLSS_EXT.1.4 Test #1a	211
7.5.7	FCS_DTLSS_EXT.1.4 Test #1b	211
7.5.8	FCS_DTLSS_EXT.1.4 Test #2	212
7.5.9	FCS_DTLSS_EXT.1.4 Test #3	212
7.5.10	FCS_DTLSS_EXT.1.5 Test #1	213
7.5.11	FCS_DTLSS_EXT.1.6 Test #1	214
7.5.12	FCS_DTLSS_EXT.1.7 Test #1	214
7.5.13	FCS_DTLSS_EXT.1.7 Test 2a	215
7.5.14	FCS_DTLSS_EXT.1.7 Test 2b	216
7.5.15	FCS_DTLSS_EXT.1.7 Test 3a	216
7.5.16	FCS_DTLSS_EXT.1.7 Test 3b	216
<b>7.6</b>	<b>DTLSS-MA</b>	<b>217</b>
7.6.1	FCS_DTLSS_EXT.2.1&2.2 Test #1a	217
7.6.2	FCS_DTLSS_EXT.2.1&2.2 Test #1b	217
7.6.3	FCS_DTLSS_EXT.2.1&2.2 Test #2	218
7.6.4	FCS_DTLSS_EXT.2.1&2.2 Test #3	218
7.6.5	FCS_DTLSS_EXT.2.1&2.2 Test #4	219
7.6.6	FCS_DTLSS_EXT.2.1&2.2 Test #5a	219
7.6.7	FCS_DTLSS_EXT.2.1&2.2 Test #5b	220
7.6.8	FCS_DTLSS_EXT.2.1&2.2 Test #6	220
7.6.9	FCS_DTLSS_EXT.2.1&2.2 Test #7	221
7.6.10	FCS_DTLSS_EXT.2.1&2.2 Test #8	222
7.6.11	FCS_DTLSS_EXT.2.3 Test #1	222
<b>7.7</b>	<b>DTLSC</b>	<b>222</b>



7.7.1	FCS_DTLSC_EXT.1.1 Test #1	222
7.7.2	FCS_DTLSC_EXT.1.1 Test #2	224
7.7.3	FCS_DTLSC_EXT.1.1 Test #3	225
7.7.4	FCS_DTLSC_EXT.1.1 Test #4a	225
7.7.5	FCS_DTLSC_EXT.1.1 Test #4b	226
7.7.6	FCS_DTLSC_EXT.1.1 Test #4c	226
7.7.7	FCS_DTLSC_EXT.1.1 Test #5a	226
7.7.8	FCS_DTLSC_EXT.1.1 Test #5b	227
7.7.9	FCS_DTLSC_EXT.1.1 Test #6a	227
7.7.10	FCS_DTLSC_EXT.1.1 Test #6b	228
7.7.11	FCS_DTLSC_EXT.1.1 Test #6c	228
7.7.12	FCS_DTLSC_EXT.1.2 Test #1	229
7.7.13	FCS_DTLSC_EXT.1.2 Test #2	230
7.7.14	FCS_DTLSC_EXT.1.2 Test #3	232
7.7.15	FCS_DTLSC_EXT.1.2 Test #4	234
7.7.16	FCS_DTLSC_EXT.1.2 Test #5 (1)	235
7.7.17	FCS_DTLSC_EXT.1.2 Test #5 (2)(a)	236
7.7.18	FCS_DTLSC_EXT.1.2 Test #5 (2)(b)	238
7.7.19	FCS_DTLSC_EXT.1.2 Test #5 (2)(c)	239
7.7.20	FCS_DTLSC_EXT.1.2 Test #6	240
7.7.21	FCS_DTLSC_EXT.1.2 Test #7a	242
7.7.22	FCS_DTLSC_EXT.1.2 Test #7b	243
7.7.23	FCS_DTLSC_EXT.1.2 Test #7c	244
7.7.24	FCS_DTLSC_EXT.1.2 Test #7d	245
7.7.25	FCS_DTLSC_EXT.1.3 Test #1	246
7.7.26	FCS_DTLSC_EXT.1.3 Test #2	247
7.7.27	FCS_DTLSC_EXT.1.3 Test #3	247
7.7.28	FCS_DTLSC_EXT.1.4 Test #1	248
7.7.29	FCS_DTLSC_EXT.2.1 Test #1	248
7.7.30	FCS_DTLSC_EXT.2.2 Test #1	249
7.7.31	FCS_DTLSC_EXT.2.3 Test #1	249
<b>7.8</b>	<b>SSHC</b>	<b>250</b>
7.8.1	FCS_SSHC_EXT.1.2 Test #1	250
7.8.2	FCS_SSHC_EXT.1.2 Test #2	251
7.8.3	FCS_SSHC_EXT.1.3 Test #1	251
7.8.4	FCS_SSHC_EXT.1.4 Test #1	251
7.8.5	FCS_SSHC_EXT.1.5 Test #1	252
7.8.6	FCS_SSHC_EXT.1.5 Test #2	253
7.8.7	FCS_SSHC_EXT.1.6 Test #1	253
7.8.8	FCS_SSHC_EXT.1.6 Test #2	254
7.8.9	FCS_SSHC_EXT.1.7 Test #1	254
7.8.10	FCS_SSHC_EXT.1.8 Test #1t	255

7.8.11	FCS_SSHC_EXT.1.8 Test #1b	256
7.8.12	FCS_SSHC_EXT.1.9 Test #1	257
7.8.13	FCS_SSHC_EXT.1.9 Test #2	257
<b>7.9</b>	<b>SHSS</b>	<b>258</b>
7.9.1	FCS_SSHS_EXT.1.2 Test #1	258
7.9.2	FCS_SSHS_EXT.1.2 Test #2	259
7.9.3	FCS_SSHS_EXT.1.2 Test #3	259
7.9.4	FCS_SSHS_EXT.1.2 Test #4	260
7.9.5	FCS_SSHS_EXT.1.3 Test #1	260
7.9.6	FCS_SSHS_EXT.1.4 Test #1	260
7.9.7	FCS_SSHS_EXT.1.5 Test #1	261
7.9.8	FCS_SSHS_EXT.1.5 Test #2	262
7.9.9	FCS_SSHS_EXT.1.6 Test #1	262
7.9.10	FCS_SSHS_EXT.1.6 Test #2	263
7.9.11	FCS_SSHS_EXT.1.7 Test #1	264
7.9.12	FCS_SSHS_EXT.1.7 Test #2	264
7.9.13	FCS_SSHS_EXT.1.8 Test #1t	265
7.9.14	FCS_SSHS_EXT.1.8 Test #1b	266
<b>7.10</b>	<b>TLSS</b>	<b>267</b>
7.10.1	FCS_TLSS_EXT.1.1 Test #1	267
7.10.2	FCS_TLSS_EXT.1.1 Test #2	269
7.10.3	FCS_TLSS_EXT.1.1 Test #3a	269
7.10.4	FCS_TLSS_EXT.1.1 Test #3b	269
7.10.5	FCS_TLSS_EXT.1.2 Test #1	270
7.10.6	FCS_TLSS_EXT.1.3 Test #1a	271
7.10.7	FCS_TLSS_EXT.1.3 Test #1b	271
7.10.8	FCS_TLSS_EXT.1.3 Test #2	271
7.10.9	FCS_TLSS_EXT.1.3 Test #3	272
7.10.10	FCS_TLSS_EXT.1.4 Test #1	272
7.10.11	FCS_TLSS_EXT.1.4 Test #2a	273
7.10.12	FCS_TLSS_EXT.1.4 Test #2b	274
7.10.13	FCS_TLSS_EXT.1.4 Test #3a	275
7.10.14	FCS_TLSS_EXT.1.4 Test #3b	276
<b>7.11</b>	<b>Firewall</b>	<b>276</b>
7.11.1	FFW_RUL_EXT.1 Test #1	276
7.11.2	FFW_RUL_EXT.1 Test #2	277
7.11.3	FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Test #1	278
7.11.4	FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Test #2	282
7.11.5	FFW_RUL_EXT.1.5 Test #1	283
7.11.6	FFW_RUL_EXT.1.5 Test #2	285

7.11.7	FFW_RUL_EXT.1.5 Test #3	286
7.11.8	FFW_RUL_EXT.1.5 Test #4	286
7.11.9	FFW_RUL_EXT.1.5 Test #5	288
7.11.10	FFW_RUL_EXT.1.5 Test #6	288
7.11.11	FFW_RUL_EXT.1.5 Test #7	290
7.11.12	FFW_RUL_EXT.1.5 Test #8	291
7.11.13	FFW_RUL_EXT.1.6 Test #1	292
7.11.14	FFW_RUL_EXT.1.6 Test #2	295
7.11.15	FFW_RUL_EXT.1.7 Test #1	295
7.11.16	FFW_RUL_EXT.1.7 Test #2	296
7.11.17	FFW_RUL_EXT.1.8 Test #1	298
7.11.18	FFW_RUL_EXT.1.8 Test #2	299
7.11.19	FFW_RUL_EXT.1.9 Test #1	300
7.11.20	FFW_RUL_EXT.1.10 Test #1	300
<b>7.12</b>	<b>Update</b>	<b>301</b>
7.12.1	FPT_TST_EXT.1 Test #1	301
7.12.2	FPT_TST_EXT.2 Test #1	302
7.12.3	FPT_TUD_EXT.1 Test #1	302
7.12.4	FPT_TUD_EXT.1 Test #2 (a)	303
7.12.5	FPT_TUD_EXT.1 Test #2 (b)	303
7.12.6	FPT_TUD_EXT.1 Test #2 (c)	304
7.12.7	FPT_TUD_EXT.1 Test #3 (a)	305
7.12.8	FPT_TUD_EXT.1 Test #3 (b)	306
<b>8</b>	<b>CAVP Algorithm Certificate Details</b>	<b>307</b>
<b>9</b>	<b>Conclusion</b>	<b>309</b>

## 1 TOE Overview


The TOE is KlasOS Keel 5.4.0 running on the VoyagerVMm, TRX R2 and Voyager VM3.0 platforms (herein referred to as the TOE). It runs the KlasOS Keel 5.4.0 firmware combining both connectivity and local compute capabilities. Network connectivity includes ethernet and SDWAN. Computing and firewall capabilities are combined in one unit. This provides users with cloud connectivity when necessary and local processing power for analytics when there is no backhaul. Administration can be performed locally or over a trusted SSH channel.

### 1.1 TOE Description

This Section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references. All TOE models below run the same Klas Keel 5.4.0 binary file.

Table 1 – TOE Models

TOE Model	Specifications
VoyagerVMm (i3) and VoyagerVMm (i5) 	5 <sup>th</sup> Gen Intel® Dual Core i3-5010U (1.8 GHz) Broadwell-U, 8 GB DDR3 RAM Network Ports: 1 x console, 4 x Gb Ethernet Storage: Samsung 850 EVO 256 GB mSATA SSD or Samsung 1TB mSATA SSD
	5 <sup>th</sup> Gen Intel® Quad Core i5-5350U (1.8 GHz) Broadwell-U, 32 GB DDR3 RAM Network Ports: 1 x console, 4 x Gb Ethernet Storage: Samsung 850 EVO 256 GB mSATA SSD or Samsung 1TB mSATA SSD
TRX R2 (4-core) and TRX R2 (8-core) 	Atom™/Denverton C3508 Intel® Atom™ Denverton C3508 4-Core processor with 1.6 GHz clock. 8 GB RAM (upgradeable to 32 GB) Network Ports: 2 x 1 Gb Ethernet 4G/LTE Modems Sierra Wireless EM7455 LTE Cat-6 (B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B29, B30, B41) Sierra Wireless EM7511 LTE Cat-12 (B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B26, B29, B30, B32, B41, B42, B43, B46, B48, B66) IEEE802.11 ac/b/g/n 3x3 MIMO Wi-Fi modem with data rates of 1.3 Gb/s downlink in 2.4/5 Ghz bands
	Atom™/Denverton C3708 Intel® Atom™ Denverton C3708 8-Core processor with 1.7 GHz clock. 8 GB RAM (upgradeable to 32 GB) Network Ports: 2 x 1 Gb Ethernet 4G/LTE Modems

TOE Model	Specifications
	<p>Sierra Wireless EM7455 LTE Cat-6 (B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B29, B30, B41)</p> <p>Sierra Wireless EM7511 LTE Cat-12 (B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B26, B29, B30, B32, B41, B42, B43, B46, B48, B66)</p> <p>IEEE802.11 ac/b/g/n 3x3 MIMO Wi-Fi modem with data rates of 1.3 Gb/s downlink in 2.4/5 Ghz bands</p>
<p>VoyagerVM 3.0</p> 	<p>Xeon D-1539</p> <p>Intel® Xeon Processor D1539 16-Core with 48 or 96 GB RAM</p> <p>Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet.</p> <p>Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)</p> <hr/> <p>Xeon D-1559</p> <p>Intel® Xeon Processor D1559 12-Core with 48 or 96 GB RAM</p> <p>Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet.</p> <p>Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)</p> <hr/> <p>Xeon D-1577</p> <p>Intel® Xeon Processor D1577 16-Core with 48 or 96 GB RAM</p> <p>Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet.</p> <p>Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)</p>

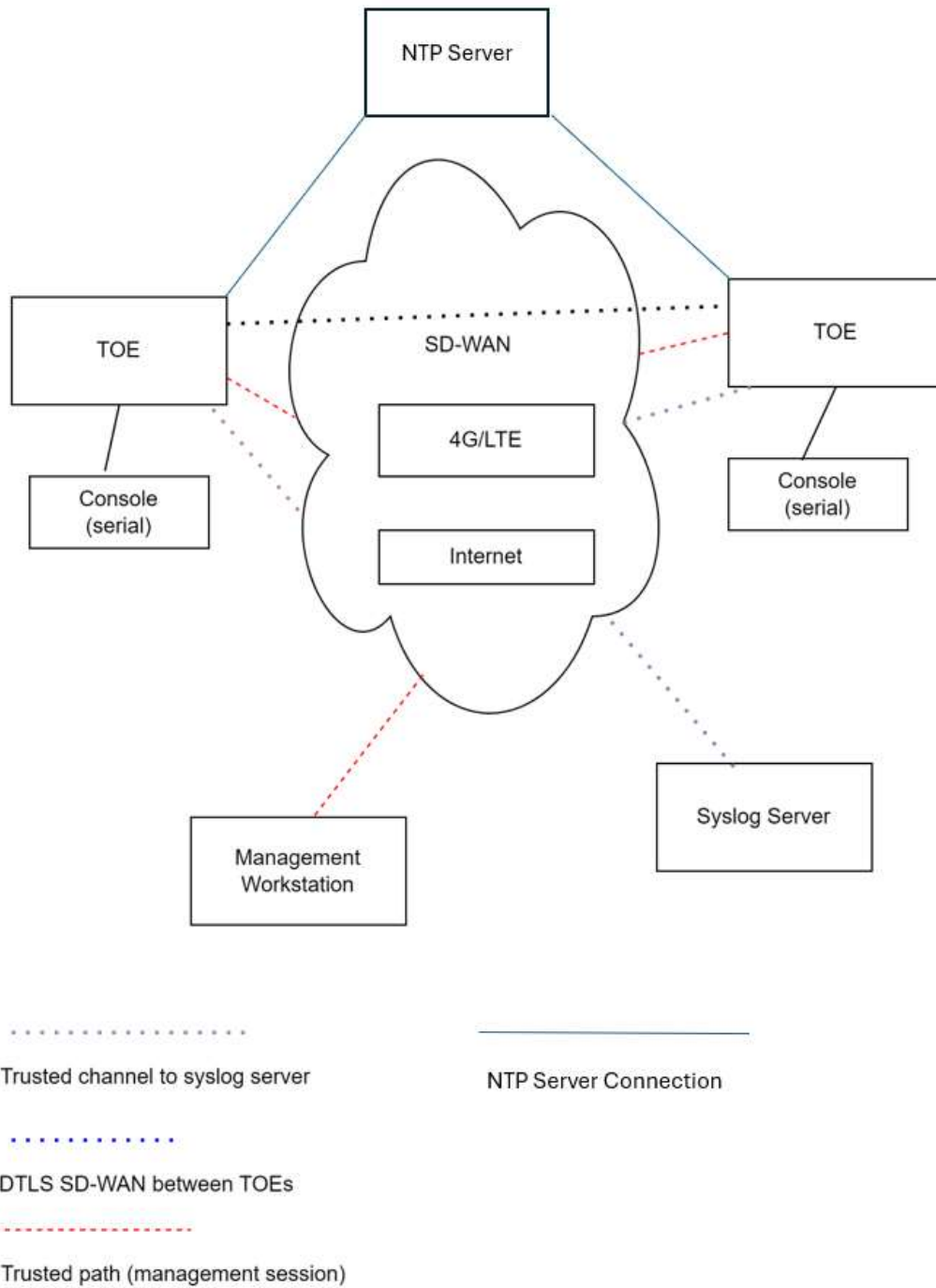


Figure 1 – Representative TOE Deployment

### 1.1.1 Physical Boundaries

The TOE boundary is the hardware appliance which is comprised of hardware and the KlasOS Keel software component. This Section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references. All TOE models below run the same Klas Keel 5.4.0 binary file.

Table 1 – TOE Models.

The TOE also supports connection to one or more TOEs over an SD-WAN, which is protected by DTLS. In the evaluated configuration, this connection is used solely for the administration of another TOE using SSH over the SD-WAN connection.

The TOE also supports secure connectivity with several other IT environment devices, including the ones identified in the following table.

The TOE implements HTTPS as a limited functionality GUI back to the management workstation. The GUI only offers basic monitoring capabilities and is secured via TLS when an administrator is logged in. Peer certificates are not required for authentication.

**Table 2 – IT Environment Components**

Component	Required	Purpose/Description
Local Management Workstation	Yes	A management workstation that is directly connected to the TOE's console port may be used by the TOE administrator to support TOE administration.
Remote Management Workstation / SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channel. Any SSH client that supports SSHv2 may be used. This remote management station is also utilized to access the TOE's HTTPS GUI for monitoring capabilities.
Syslog Server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. An SSH tunnel is established by the TOE and logs are transmitted using this encrypted method.
NTP Server	No	The NTP server is used to send reliable timestamps to the TOE using NTPv3 and SHA1 as the message digest algorithm.

## **2 Assurance Activities Identification**

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e and MOD\_CPP\_FW\_V1.4E based upon the core SFRs and those implemented based on selections within the PP.



### 3 Test Equivalency Justification

The TOE is KlasOS Keel5.4.0 running on the VoyagerVMm, TRX R2 and Voyager VM3.0 platforms (herein referred to as the TOE). It runs the KlasOS Keel 5.4.0 firmware combining both connectivity and local compute capabilities. Network connectivity includes ethernet and SDWAN. Computing and firewall capabilities are combined in one unit. This provides users with cloud connectivity when necessary and local processing power for analytics when there is no backhaul. Administration can be performed locally or over a trusted SSH channel.

#### 3.1 Architectural Description

All the possible TOE chassis are listed below:

- Klas VoyagerVMm
- Klas TRX R2
- Klas VoyagerVM3.0

##### 3.1.1 Klas TRXr2

The software is comprised of the Klas Keel 5.4.0 and is consistent across all 3 platforms. Architecture for the Klas TRXr2 uses the processor family of Intel Atom and the 2 models that it offered are the C3508 and the C3708. The C3508 has a total of 4 cores in the processor and has a clock speed of 1.6GHz. The C3708 has a total of 8 cores in the processor and has a clock speed of 1.7GHz.

##### 3.1.2 Klas Voyager VMm

Architecture for the Klas Voyager VMm uses the processor family of Intel Dual Core processors. The models of processors that the VMm uses are the i3 and the i5. The Dual Core i3 has 2 cores in the processor and a clock speed of 2.1GHz. The Dual Core i5 has 2 cores in the processor and a clock speed of 1.8GHz.




##### 3.1.3 Klas Voyager VM3

Architecture for the Klas Voyager VM3 uses the processor family of Intel Xeon processors. The model of processors that the VM3 uses are the D1539, D1559, and the D1577. The Xeon D1539 has 8 cores and a clock speed of 1.6GHz. The Xeon D1559 has 12 cores and a clock speed of 1.5GHz. The Xeon D1577 has 16 cores and a clock speed of 1.3ghz.

#### 3.2 Specification of Differences

The following tables provide a description of the physical differences between hardware models.

**Table 4- Hardware Models and Specifications**

Specification	Platforms		
	 <p><b>Voyager VMm</b></p>	 <p><b>TRX R2</b></p>	 <p><b>Voyager VM3.0</b></p>
Dimension HxWxD	7.4" W x 5.7" L x 1.0" H	7.4" W x 6.3" L x 2" H	7.4" W x 6.3" L x 2" H
Weight	2.2 lb / 1.0 kg	4.4 lb	3.5 lb / 1.6 kg (with no SSDs)
Processor	5 <sup>th</sup> Gen Intel® Dual Core i3-5010U (1.8 GHz) Broadwell-U Or 5 <sup>th</sup> Gen Intel® Quad Core i5-5350U (1.8 GHz) Broadwell-U	Atom™/Denverton C3508 Intel® Atom™ Denverton C3508 4-Core processor with 1.6 GHz clock or Atom™/Denverton C3708 Intel® Atom™ Denverton C3708 4-Core processor with 1.7 GHz clock	Xeon D-1539 Intel® Xeon Processor D1539 16-Core Or Xeon D-1559 Intel® Xeon Processor D1559 12-Core Or Xeon D-1577 Intel® Xeon Processor D1577 16-Core
RAM	8GB DDR3 - 32GB DDR3	8GB	48 or 96GB of RAM
Storage	Storage: Samsung 850 EVO 256 GB mSATA SSD or Samsung 1TB mSATA SSD	VIK+ NVMe removable storage (256GB or 512GB)	Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)
Power	20 W power consumption	15 - 32 W power consumption	8-core (D-1539): 55 W 12-core (D-1559): 65 W 16-core (D-1577): 65 W
DC Voltage	Power: 10-18 VDC Input	9 - 36 VDC input	9-36 VDC Input
Network Card	1 x console, 4 x Gb Ethernet	Network Ports: 2 x 1 Gb Ethernet 4G/LTE Modems Sierra Wireless EM7455 LTE Cat-6 (B1, B2, B3, B4, B5, B7, B12,	Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet

Specification	Platforms		
		B13, B20, B25, B26, B29, B30, B41) Sierra Wireless EM7511 LTE Cat-12 (B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B26, B29, B30, B32, B41, B42, B43, B46, B48, B66) IEEE802.11 ac/b/g/n 3x3 MIMO Wi-Fi modem with data rates of 1.3 Gb/s downlink in 2.4/5 Ghz bands	
Temperature	32°F – 122°F	32°F – 122°F	32°F – 95°F
Humidity	5% – 95%	5% – 95%	5% – 95%

### 3.3 Equivalency Analysis

The following equivalency analysis provides a per category analysis of key areas of differentiation for each appliance to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the NDcPP v2.2E.

#### 3.3.1 Platform/Hardware Dependencies

Since the HW platforms do not provide any of the TSF functionality, no hardware is included in the TOE boundary. All security functionality is implemented in platform-independent code which is the same operating system (Klas Keel 5.4.0) across all hardware models. There are no platform or hardware-specific dependencies of the TOE.

Result: All TOE platforms are equivalent

#### 3.3.2 Differences in Libraries Used to Provide TOE Functionality

All 3 devices have the same software installed across all claimed hardware platforms. Of note, the TOE uses the same CAVP validated crypto modules to provide its cryptographic functionality. This is the same across platforms.

Result: All platforms are equivalent

#### 3.3.3 TOE Management Interface Differences

The TOE is managed via either remote CLI session or directly connected CLI. These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.

Result: All platforms are equivalent

### 3.3.4 TOE Functional Differences

Each hardware model within the TOE boundary provides identical functionality. There is no difference in the way the user interacts with each of the devices or the services that are available to the user in for each of these TOE's models. Each TOE's model can be run with the same identical version of Klas Keel 5.4.0 operating system.

Result: All TOE platforms are equivalent

#### **Security Audit**

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in Table 13 – Security Functional Requirements and Auditable Events(ST). Audit events are also generated for management actions specified in FAU\_GEN.1. The TOE stores audit records locally and can export them to an external syslog server using SSHv2. Each audit record contains the data and time of the event, type of event, subject identity, and other relevant data for the event. Only a security administrator can enable logging to a syslog server. Each TOE model executes the identical Klas Keel binary image.

Result: All TOE platforms are equivalent

#### **Cryptographic Support**

The Klas Keel 5.4.0 OS uses OpenSSL version 3.0.8 to enforce all cryptographic support. Each TOE model executes an identical Klas Keel binary image. All software binaries compiled in the TOE software are identical and have the same version numbers. CAVP certificate #A4573 has been issued for the cryptographic support of the TOE tested processors.

Result: All TOE platforms are equivalent

#### **Identification & Authentication**

All users must be authenticated by the TOE prior to carrying out any administrative actions. The TOE supports password-based and public-key based authentication. An administrator can set a minimum password length on the TOE which must be at least 15 characters. This is true of users accessing the TOE via the local console, or through protected paths using the remote CLI via SSH. Users can authenticate to the TOE using a username and password. In addition, when authenticating by the remote CLI, users can instead use SSH public-key authentication. Passwords can consist of upper-case letters, lower-case letters, numbers, and a set of selected special characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates the device, a customizable warning banner is configured to be displayed. The TSF determines the validity of the certificates by confirming the validity of the certificate chain and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TSF connects with an OCSP responder through an OCSP responder link in the certificate to confirm certificate validity.

#### **Security Management**

All TOE models support local and remote management of its security functions including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Configurable banner displayable at login
- Timeouts to terminate administrative sessions after a set period of inactivity.
- Timed user lockout after multiple failed authentication attempts
- Configurable authentication failure parameters
- Re-enabling locked accounts.
- Configurable cryptographic parameters

The administrative user can perform all the above security-related management functions.

Result: All TOE platforms are equivalent

#### **Protection of the TSF**

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Passwords are stored as SHA 512 hashes. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. The TOE internally maintains the date and time. An administrator can install software updates to the TOE after they are verified using a digital signature mechanism.

Result: All TOE platforms are equivalent

### TOE Access

The TOE displays a customizable banner before any administrative session can be established with it. The TOE will terminate local or remote interactive sessions after a specified period of session inactivity configured by an administrator. An administrator can terminate their own interactive local or remote sessions.

The local and remote CLI interfaces display the default security banner prior to authentication that is also configurable. The TOE can terminate local CLI and remote CLI sessions after a specified time-period of inactivity. Administrative users have the capability to terminate their own sessions.

Result: All TOE platforms are equivalent

### Trusted Path/Channels

The TOE supports SSH for secure communications with authorized IT entities such as syslog servers. The TOE supports SSHv2 (remote CLI) for secure remote administration. The TOE also supports DTLS for secure communication between TOEs to support SD-WAN.

Result: All TOE platforms are equivalent

### Conclusion:

All platforms are equivalent and provide the same TOE Security Functionality. A full suite of testing will be performed on devices listed below:

- Klas Voyager VMm
  - Intel® Dual Core i5-5350U (1.8 GHz) Broadwell-U
- Klas TRX R2
  - Atom Denverton C3508 4-Core processor with 1.6 GHz clock
- Klas VoyagerVM3.0
  - Xeon D-1539 16-Core

### 3.3.5 Difference Comparison based on CPU micro-architecture

The subsequent table provides a comparison of the Operating System, CPU Micro-architecture, CPU, Instruction Set Extensions, CPU Family, Hardware Reference, and Model that operate on each of the included TOE platforms. All systems will be associated with an identical set of CAVP certificates. There are differences in the Instruction Set Extensions and the CPU families, but they are purely performance related not security related.

TOE's Model	TOE's OS version	Instruction Set Extensions	CPU	CPU Family	CPU Micro-architecture
TRXr2	3.3.6 Klas Keel OS 5.4.0	64-bit	Intel Atom c3508	Atom c3000 series	Goldmont
TRXr2	Klas Keel OS 5.4.0	64-bit	Intel Atom c3708	Atom c3000 series	Goldmont
Voyager VMm	Klas Keel OS 5.4.0	Intel SSE4.1, Intel SSE4.2, Intel AVX2	Intel Core i3-5010U	5 <sup>th</sup> Gen Core i3	Broadwell
Voyager VMm	Klas Keel OS 5.4.0	Intel SSE4.1, Intel SSE4.2, Intel AVX2	Intel Core i5-5350U	5 <sup>th</sup> Gen Core i5	Broadwell

Voyager VM3	Klas Keel OS 5.4.0	Intel AVX2	Intel Xeon D-1539	Xeon D	Broadwell
Voyager VM3	Klas Keel OS 5.4.0	Intel AVX2	Intel Xeon D-1559	Xeon D	Broadwell
Voyager VM3	Klas Keel OS 5.4.0	Intel AVX2	Intel Xeon D-1577	Xeon D	Broadwell

### 3.3.7 Difference Comparison based on CPU Security features.

The subsequent table provides a comparison of the security features of all of the TOE models and their associated processors. The Voyager VMm with the Intel Core i5-5350u is equipped with Intel vPro Technology which is an umbrella marketing term that involved VT-x, VT-d, trusted execution Technology and Intel Active Management Technology.

#### CPU Security Features

TOE model and processor	(TRXr2) Intel Atom c3508	(TRXr2) Intel Atom c3708	(VoyagerVMm) Intel Core i3-5010U	(Voyager VMm) Intel Core i5-5350U	(Voyager VM3) Intel Xeon D1539	(Voyager VM3) Intel Xeon D1559	(VoyagerVM3) Intel Xeon D1577
Intel vPro Technology	No	No	No	Yes	No	No	No
Intel AES New Instructions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Secure Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel SGx	No	No	No	No	No	No	No
Intel Execute Disable Bit	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel OS Guard	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Boot Guard	No	No	No	No	No	No	No
Intel Virtualization Technology	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Virtualization Technology for Directed I/O	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel VT-x with Extended Page Tables	Yes	Yes	Yes	Yes	Yes	Yes	Yes

### 3.4 Recommendations/Conclusions

Based on the equivalency rationale listed above, the main differences are:

- Performance differences in the CPU architecture for each TOE model.

All hardware devices in this evaluation compile and execute the same binary update file of Klas Keel 5.4.0. Because of this, all platforms are equivalent between processor families and provide the same TOE Security Functionality. A full suite of testing will be performed on devices listed below:

- Klas Voyager VMm
  - Intel® Dual Core i5-5350U (1.8 GHz) Broadwell-U
- Klas TRX R2
  - Atom Denverton C3508 4-Core processor with 1.6 GHz clock
- Klas VoyagerVM3.0
  - Xeon D-1539 16-Core

### 3.5 References

The current equivalency report draws references from the following web links:

1. [Intel Atom Comparison](#) – This Intel web link is utilized to compare the specifications of the Intel Atom c3508 and Intel Atom c3708.
2. [Intel Core processors Comparison](#) – This Intel web link is utilized to compare the specifications of the Intel Core i3-5010u and the Intel Core i5-5350u.
3. [Intel Xeon processor comparison](#) – This Intel web link is utilized to compare the specifications of the Intel Xeon D1539, Intel Xeon D1559, and the Intel Xeon D1577.
4. [Intel vPro definition](#) – This Wikipedia link is utilized to define the Intel vPro technology.

### 3.6 Appendix: Processor Technical Comparison

#### 3.6.1 Klas TRXr2

The following table presents a technical comparison of the Intel Atom c3508 and Atom c3708 processors from the Intel ARK product comparison tool, with potentially relevant differences in the Advanced Technologies and Security & Reliability categories:

Processor	Intel Atom® Processor C3508	Intel Atom® Processor C3708
Essentials		
Product Collection	Intel Atom® Processor C Series	Intel Atom® Processor C Series
Vertical Segment	Server	Server
Processor Number	C3508	C3708
Lithography	14 nm	14 nm
Use Conditions	Communications	Communications
Recommended Customer Price	\$87.75	\$224.00
CPU Specifications		
Total Cores	4	8
Total Threads	4	8
Max Turbo Frequency	1.60 GHz	1.70 GHz
Processor Base Frequency	1.60 GHz	1.70 GHz
Cache	8 MB	16 MB
Max # of UPI Links	0	0
# of QPI Links	0	0

TDP	11.5 W	17 W
Supplemental Information		
Marketing Status	Launched	Launched
Launch Date	Q3'17	Q3'17
Embedded Options Available	Yes	Yes
Product Brief	<a href="#">View now</a>	<a href="#">View now</a>
Functional Safety (FuSa) Documentation Available	-	Yes
Memory Specifications		
Max Memory Size (dependent on memory type)	256 GB	256 GB
Memory Types	DDR4: 1866	DDR4: 2133
Max # of Memory Channels	2	2
ECC Memory Supported ‡	Yes	Yes
Expansion Options		
PCI Express Revision	3	3
PCI Express Configurations ‡	x2   x4   x8	x2   x4   x8
Max # of PCI Express Lanes	8	16
I/O Specifications		
# of USB Ports	8	8
USB Revision	3	3
Total # of SATA Ports	8	16
Integrated LAN	4x2.5/1 GbE	4x10/2.5/1 GbE
Max # of SATA 6.0 Gb/s Ports	8	16
Package Specifications		
Sockets Supported	FCBGA1310	FCBGA1310
Max CPU Configuration	1	1
TCASE	90°C	85°C
Operating Temperature (Minimum)	-40 °C	-40 °C
Package Size	34 mm x 28 mm	34 mm x 28 mm
Advanced Technologies		
Intel® Turbo Boost Technology ‡	No	No
Secure Boot	Yes	Yes
Intel® Hyper-Threading Technology ‡	No	No
Instruction Set	64-bit	64-bit
Integrated Intel® QuickAssist Technology	Yes	Yes
Security & Reliability		
Intel® AES New Instructions	Yes	Yes
Secure Key	Yes	Yes
Intel® Software Guard Extensions (Intel® SGX)	No	No
Execute Disable Bit ‡	Yes	Yes
Intel® OS Guard	Yes	Yes



Intel® Boot Guard	No	No
Intel® Virtualization Technology (VT-x) ‡	Yes	Yes
Intel® Virtualization Technology for Directed I/O (VT-d) ‡	Yes	Yes
Intel® VT-x with Extended Page Tables (EPT) ‡	Yes	Yes

### 3.6.2 Klas Voyager VMm

The following table presents a technical comparison of the Intel Core i3-5010U and an Intel Core i5-5350U processors from the Intel ARK product comparison tool, with potentially relevant differences in the Advanced Technologies and Security & Reliability categories:

Processors	Intel® Core™ i3-5010U Processor	Intel® Core™ i5-5350U Processor
Essentials		
Product Collection	5th Generation Intel® Core™ i3 Processors	5th Generation Intel® Core™ i5 Processors
Vertical Segment	Mobile	Mobile
Processor Number	i3-5010U	i5-5350U
Lithography	14 nm	14 nm
Use Conditions	Industrial Commercial Temp   Embedded Broad Market Commercial Temp   PC/Client/Tablet	Industrial Commercial Temp   Embedded Broad Market Commercial Temp   PC/Client/Tablet
Recommended Customer Price	\$281.00	
CPU Specifications		
Total Cores	2	2
Total Threads	4	4
Processor Base Frequency	2.10 GHz	1.80 GHz
Cache	3 MB	3 MB
Bus Speed	5 GT/s	5 GT/s
TDP	15 W	15 W
Configurable TDP-down Base Frequency	600 MHz	600 MHz
Configurable TDP-down	10 W	9.5 W
Max Turbo Frequency	-	2.90 GHz
Intel® Turbo Boost Technology 2.0 Frequency‡	-	2.90 GHz
Supplemental Information		
Marketing Status	Discontinued	Discontinued
Launch Date	Q1'15	Q1'15
Servicing Status	End of Servicing Lifetime	End of Servicing Lifetime

End of Servicing Updates Date	Wednesday   June 30   2021	Wednesday   June 30   2021
Embedded Options Available	Yes	Yes
Memory Specifications		
Max Memory Size (dependent on memory type)	16 GB	16 GB
Memory Types	DDR3L 1333/1600 LPDDR 1333 /1600	DDR3L 1333/1600   LPDDR3 1600/1866
Max # of Memory Channels	2	2
Max Memory Bandwidth	25.6 GB/s	25.6 GB/s
GPU Specifications		
Processor Graphics ‡	Intel® HD Graphics 5500	Intel® HD Graphics 6000
Graphics Base Frequency	300 MHz	300 MHz
Graphics Max Dynamic Frequency	900 MHz	1.00 GHz
Graphics Video Max Memory	16 GB	16 GB
Graphics Output	eDP/DP/HDMI	eDP/DP/HDMI
Max Resolution (HDMI)‡	2560x1600@60Hz	2560x1600@60Hz
Max Resolution (DP)‡	3840x2160@60Hz	3840x2160@60Hz
Max Resolution (VGA)‡	N/A	
DirectX* Support	11.2/12	11.2/12
OpenGL* Support	4.3	4.3
Intel® Quick Sync Video	Yes	Yes
Intel® InTru™ 3D Technology	Yes	Yes
Intel® Flexible Display Interface (Intel® FDI)	Yes	Yes
Intel® Clear Video HD Technology	Yes	Yes
Intel® Clear Video Technology	Yes	Yes
# of Displays Supported ‡	3	3
Device ID	0x1616	0x1626
Expansion Options		
PCI Express Revision	2	2
PCI Express Configurations ‡	4x1 2x4	4x1   2x4
Max # of PCI Express Lanes	12	12

Package Specifications		
Sockets Supported	FCBGA1168	FCBGA1168
Max CPU Configuration	1	1
TJUNCTION	105°C	105°C
Package Size	40mm x 24mm x 1.3mm	40mm x24mm x 1.3mm
Advanced Technologies		
Intel® Turbo Boost Technology ‡	No	2
Intel® Hyper-Threading Technology ‡	Yes	Yes
Intel® Transactional Synchronization Extensions	No	Yes
Intel® 64 ‡	Yes	Yes
Instruction Set	64-bit	64-bit
Instruction Set Extensions	Intel® SSE4.1   Intel® SSE4.2   Intel® AVX2	Intel® SSE4.1   Intel® SSE4.2   Intel® AVX2
Idle States	Yes	Yes
Enhanced Intel SpeedStep® Technology	Yes	Yes
Thermal Monitoring Technologies	Yes	Yes
Intel® Fast Memory Access	Yes	Yes
Intel® Flex Memory Access	Yes	Yes
Intel® Identity Protection Technology ‡	Yes	Yes
Intel® Smart Response Technology	Yes	Yes
Security & Reliability		
Intel® AES New Instructions	Yes	Yes
Secure Key	Yes	Yes
Intel® Trusted Execution Technology ‡	No	Yes
Execute Disable Bit ‡	Yes	Yes
Intel® OS Guard	Yes	Yes
Intel® Stable IT Platform Program (SIPP)	No	Yes
Intel® Virtualization Technology (VT-x) ‡	Yes	Yes

Intel® Virtualization Technology for Directed I/O (VT-d) ‡	Yes	Yes
Intel® VT-x with Extended Page Tables (EPT) ‡	Yes	Yes
Intel vPro® Eligibility ‡	-	Intel vPro® Platform

### 3.6.3 Klas Voyager VM3

The following table presents a technical comparison of the Intel Xeon D1539, Intel Xeon D1559 Processor, and Intel an Xeon D1577 from the Intel ARK product comparison tool, with potentially relevant differences in the Advanced Technologies and Security & Reliability categories:

Processor	Intel® Xeon® Processor D-1539	Intel® Xeon® Processor D-1559	Intel® Xeon® Processor D-1577
<b>Essentials</b>			
Product Collection	Intel® Xeon® D Processor	Intel® Xeon® D Processor	Intel® Xeon® D Processor
Vertical Segment	Server	Server	Server
Processor Number	D-1539	D-1559	D-1577
Lithography	14 nm	14 nm	14 nm
Use Conditions	Industrial Commercial Temp   Industrial Extended Temp	Industrial Commercial Temp   Industrial Extended Temp	Communications
Recommended Customer Price	\$556.00	\$831.00	\$1,346.00
<b>CPU Specifications</b>			
Total Cores	8	12	16
Total Threads	16	24	32
Max Turbo Frequency	2.20 GHz	2.10 GHz	2.10 GHz
Intel® Turbo Boost Technology 2.0 Frequency‡	2.20 GHz	2.10 GHz	2.10 GHz
Processor Base Frequency	1.60 GHz	1.50 GHz	1.30 GHz
Cache	12 MB	18 MB	24 MB
TDP	35 W	45 W	45 W
<b>Supplemental Information</b>			
Marketing Status	Launched	Launched	Launched
Launch Date	Q2'16	Q2'16	Q1'16
Servicing Status	End of Servicing Updates	End of Servicing Updates	End of Servicing Updates

End of Servicing Updates Date	Saturday   December 31   2022	Saturday   December 31   2022	Saturday   December 31   2022
Embedded Options Available	Yes	Yes	Yes
Product Brief	<a href="#">View now</a>	-	-
<b>Memory Specifications</b>			
Max Memory Size (dependent on memory type)	128 GB	128 GB	128 GB
Memory Types	DDR4   DDR3	DDR4   DDR3	DDR4   DDR3
Maximum Memory Speed	2133 MHz	2133 MHz	2133 MHz
Max # of Memory Channels	2	2	2
ECC Memory Supported ‡	Yes	Yes	Yes
<b>Expansion Options</b>			
Scalability	1S Only	1S Only	1S Only
PCI Express Revision	2.0/3.0	2.0/3.0	2.0/3.0
PCI Express Configurations ‡	x4 x8 x16	x4 x8 x16	x4 x8 x16
Max # of PCI Express Lanes	32	32	32
<b>I/O Specifications</b>			
# of USB Ports	8	8	8
USB Revision	2.0/3.0	2.0/3.0	2.0/3.0
Total # of SATA Ports	6	6	6
Integrated LAN	Yes	Yes	Yes
General Purpose IO	Yes	Yes	Yes
UART	Yes	Yes	Yes
<b>Networking Specifications</b>			
Interfaces Supported	SFI   KR   KX   1000Base-T   10GBase-T	SFI   KR   KX   1000Base-T   10GBase-T	SFI   KR   KX   1000Base-T   10GBase-T
<b>Package Specifications</b>			
Sockets Supported	FCBGA1667	FCBGA1667	FCBGA1667
Max CPU Configuration	1	1	1
Operating Temperature Range	-40°C to 85°C	-40°C to 85°C	-
Operating Temperature (Maximum)	85 °C	85 °C	-
Operating Temperature (Minimum)	-40 °C	-40 °C	-
Package Size	37.5mm x 37.5mm	37.5 mm x 37.5 mm	37.5 mm x 37.5 mm

Advanced Technologies			
Intel® Turbo Boost Technology ‡	2	2	2
Intel® Hyper-Threading Technology ‡	Yes	Yes	Yes
Intel® Transactional Synchronization Extensions	Yes	Yes	Yes
Intel® 64 ‡	Yes	Yes	Yes
Instruction Set	64-bit	64-bit	64-bit
Instruction Set Extensions	Intel® AVX2	Intel® AVX2	Intel® AVX2
Idle States	Yes	Yes	Yes
Enhanced Intel SpeedStep® Technology	Yes	Yes	Yes
Thermal Monitoring Technologies	Yes	Yes	Yes
Security & Reliability			
Intel® AES New Instructions	Yes	Yes	Yes
Secure Key	Yes	Yes	Yes
Intel® Trusted Execution Technology ‡	Yes	Yes	Yes
Execute Disable Bit ‡	Yes	Yes	Yes
Intel® OS Guard	Yes	Yes	Yes
Intel® Virtualization Technology (VT-x) ‡	Yes	Yes	Yes
Intel® Virtualization Technology for Directed I/O (VT-d) ‡	Yes	Yes	Yes
Intel® VT-x with Extended Page Tables (EPT) ‡	Yes	Yes	Yes

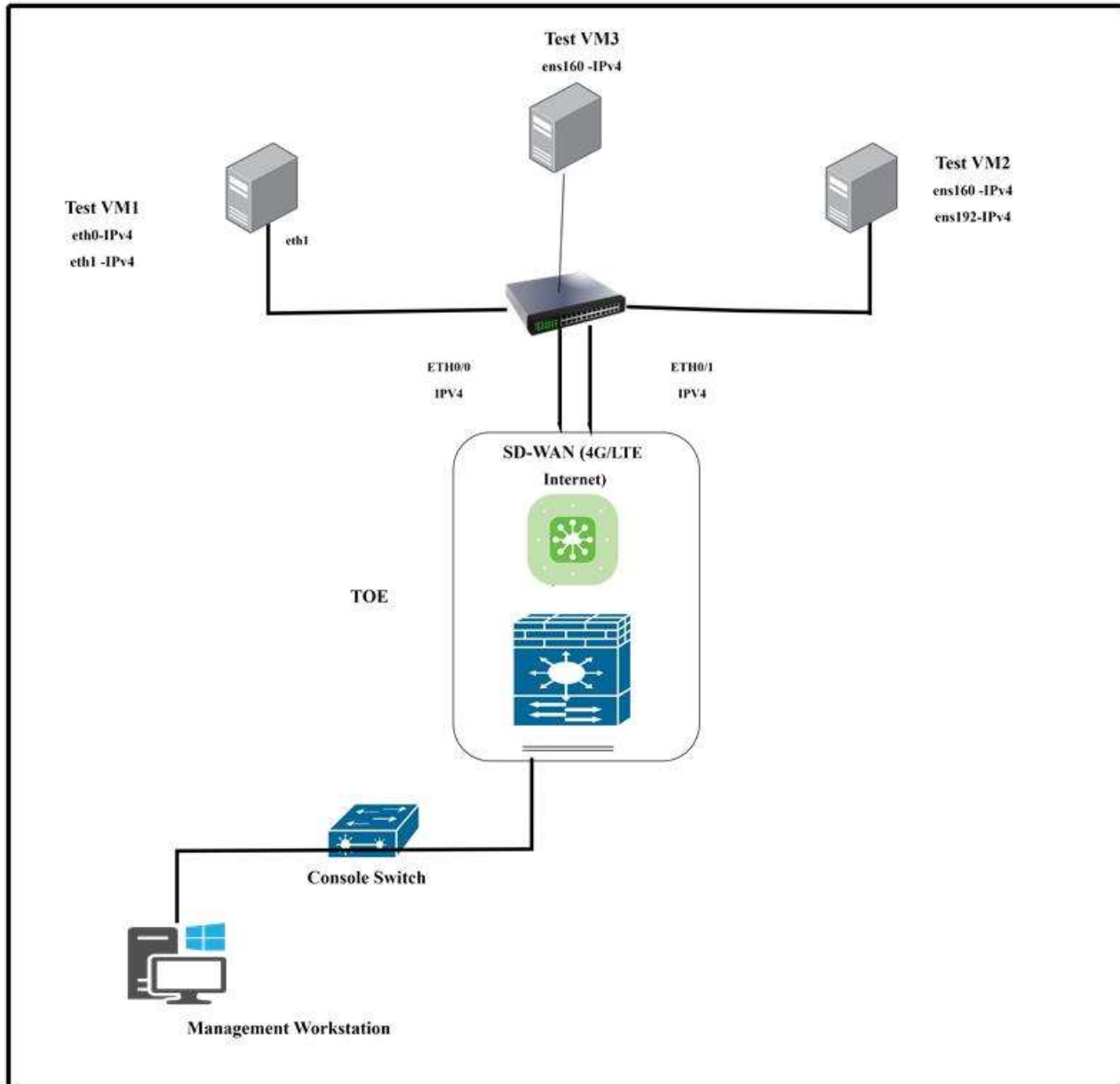
## 4 Test Bed Descriptions

### 4.1 Test Bed

Below is a visual representation of the components included in the test bed:

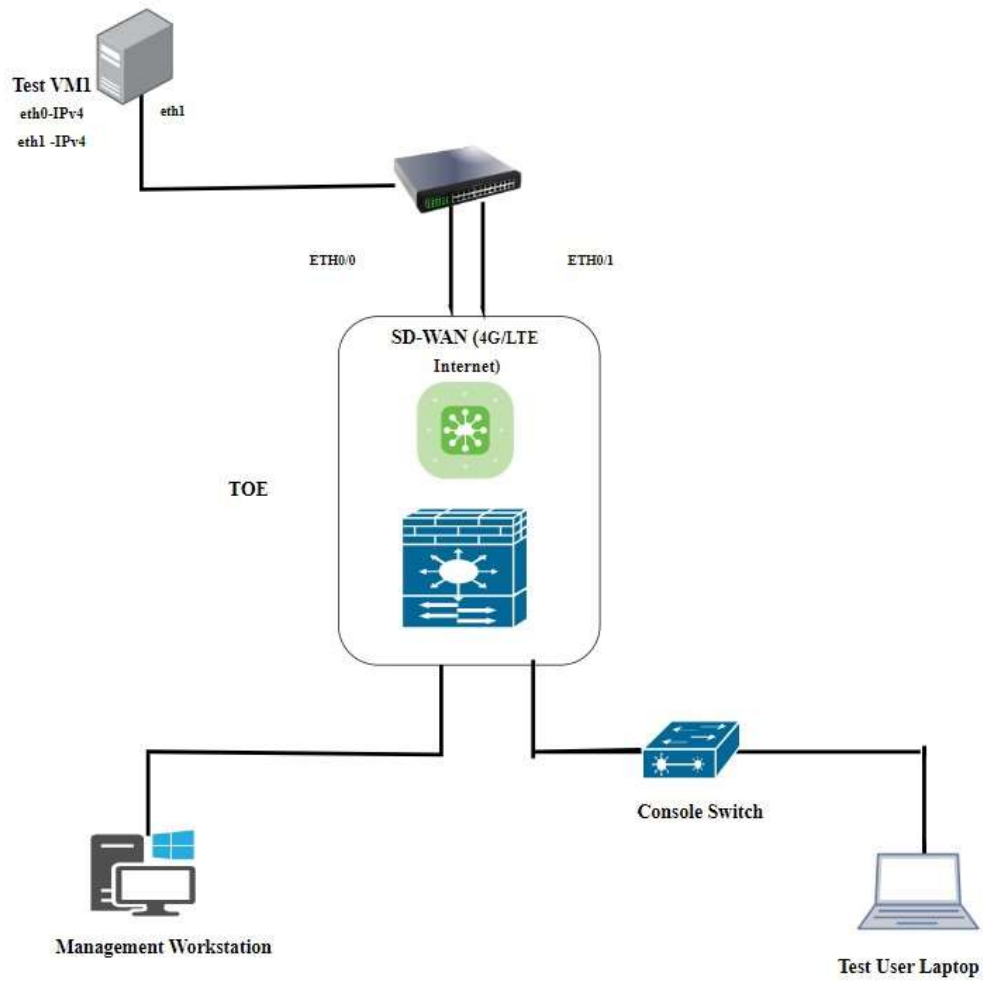
#### 4.1.1 Audit

The test bed below was used for the evaluation of the testcases for the Audit module.



### 4.1.2 Auth/Crypto/TLSS/Update

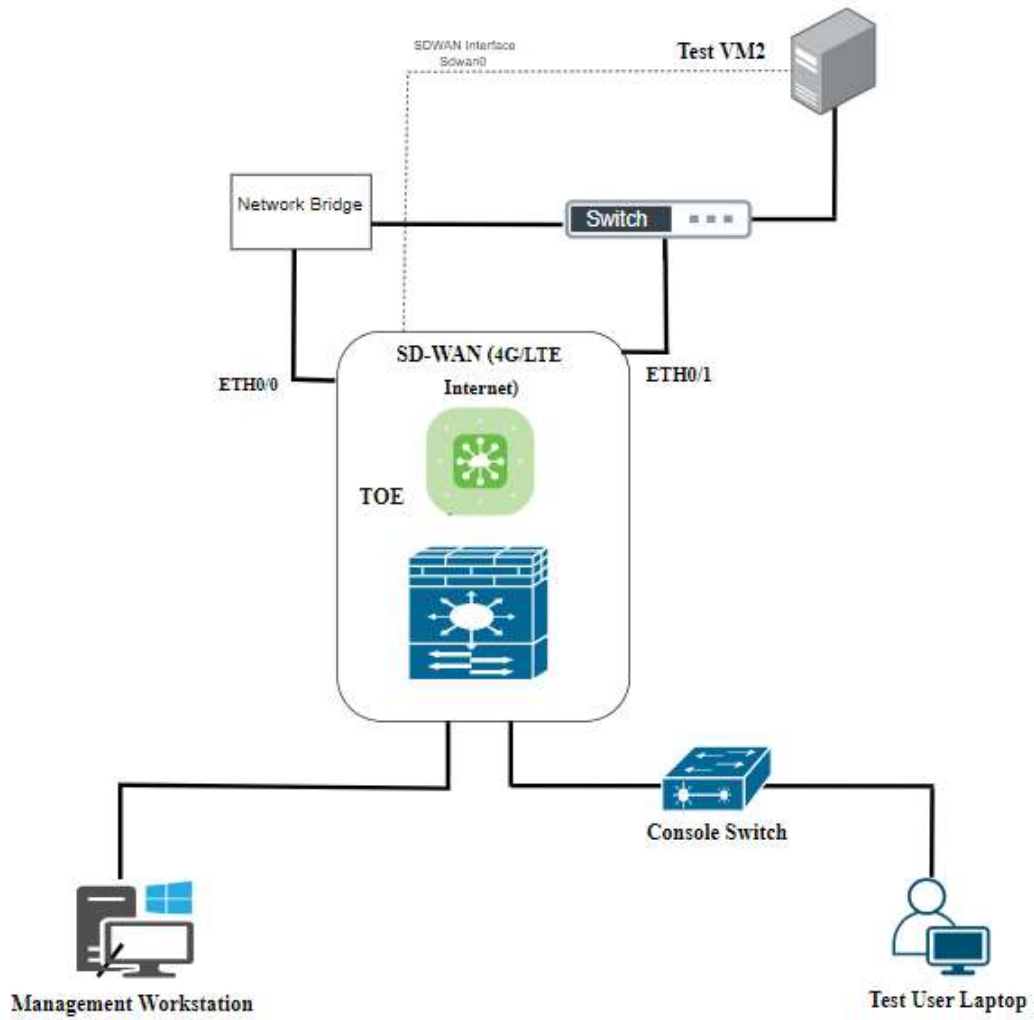
The test bed below was used for the evaluation of the testcases for the Auth/Crypto/TLSS/Update modules.





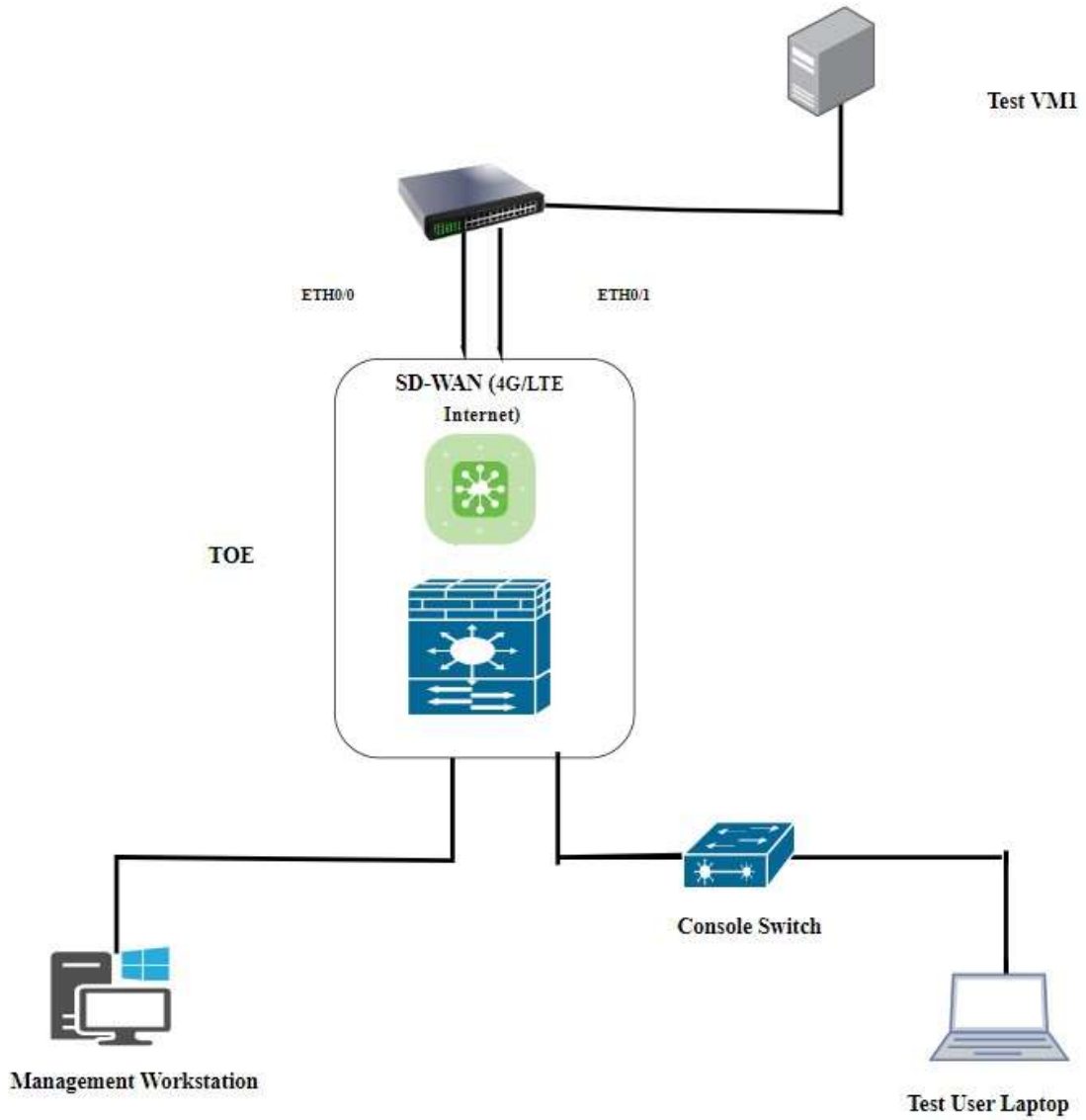
### 4.1.3 DTLS

The test bed below was used for the evaluation of the testcases for the DTLS module.



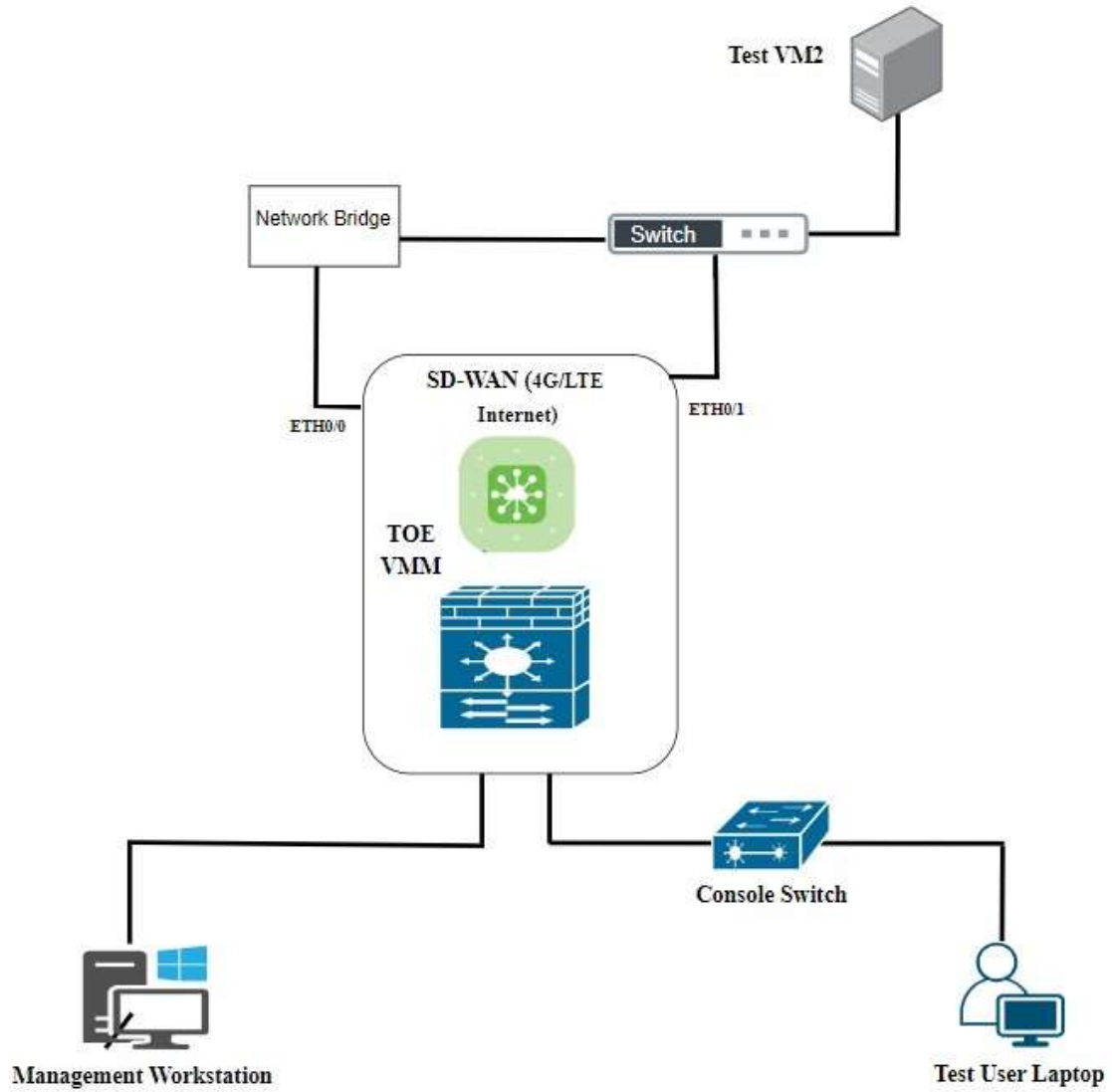
#### 4.1.4 DTLSS/X509-Rev

The test bed below was used for the evaluation of the testcases for the DTLSS/X509-Rev modules.



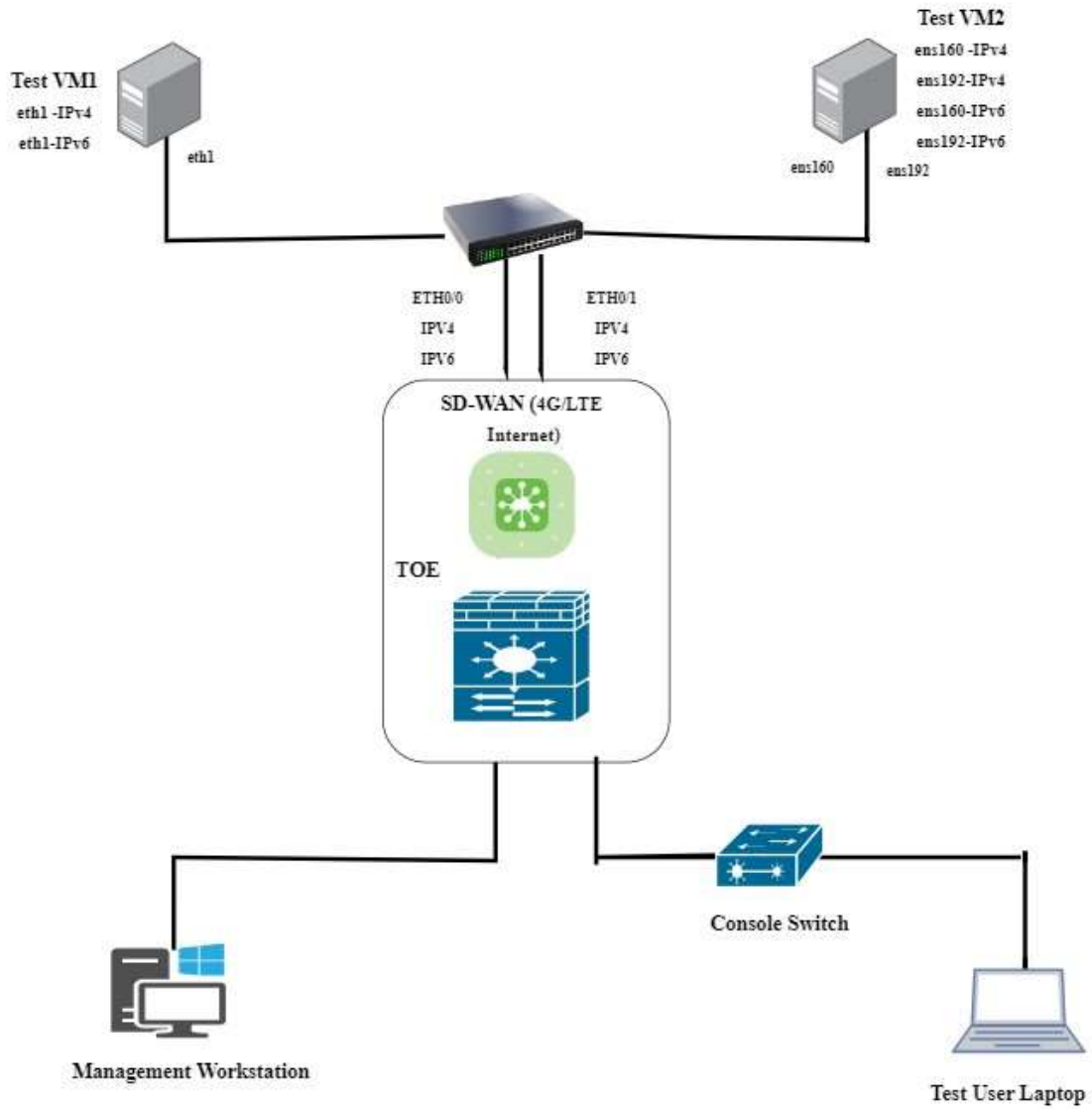
#### 4.1.5 DTLSS-MA

The test bed below was used for the evaluation of the testcases for the DTLSS-MA module.



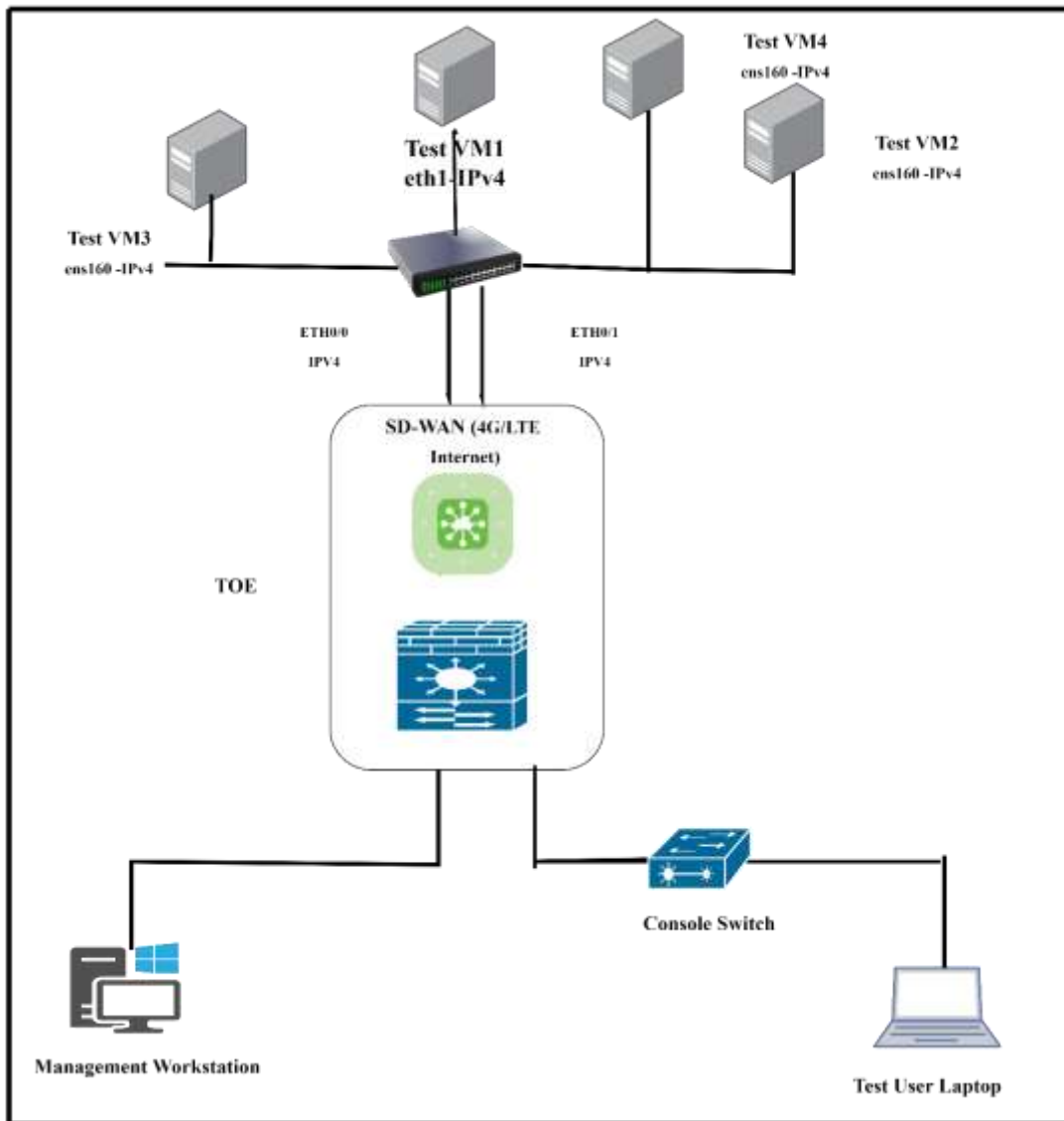
## 4.1.6 Firewall

The test bed below was used for the evaluation of the testcases for the Firewall module.



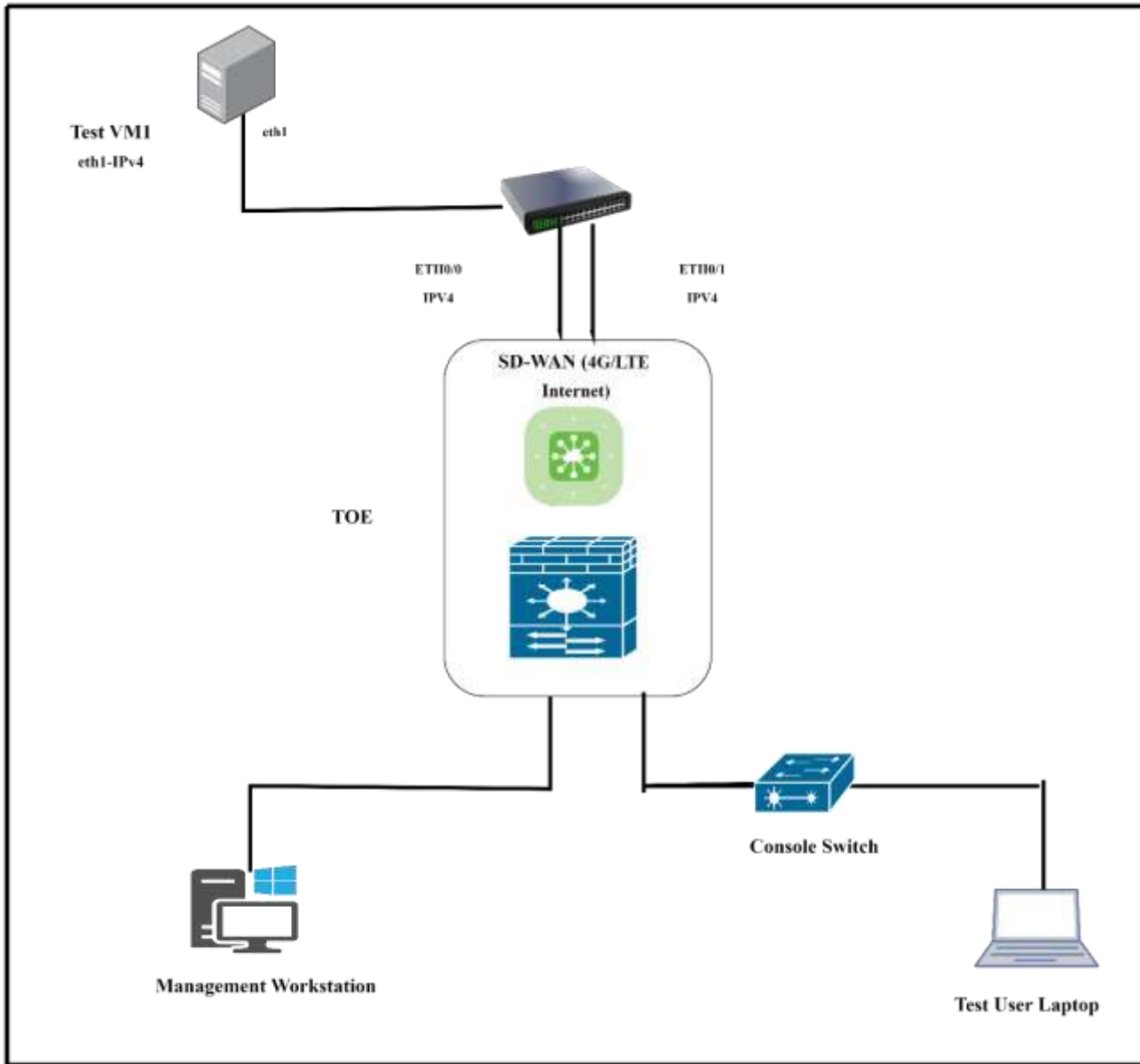
### 4.1.7 SSHC

The test bed below was used for the evaluation of the testcases for the SSHC module.



#### 4.1.8 SSHS

The test bed below was used for the evaluation of the testcases for the SSHS module.



## 4.2 Configuration Information

The following table provides configuration information about each device in the test environment.

### 4.2.1 Audit

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	DTLS DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
Test User Laptop	Tester's Laptop	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark ( 4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Kali GNU-Linux Rolling 2023.3	Manually set and verified.	openssl (1.1f) OpenSSH_9.3p2 rsyslogd 8.2308.0
Management Workstation	Remote Access	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6)
Console Switch	Console	NA	Linux Brain- Console (3.10.0-uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA

### 4.2.2 Auth/Crypto/TLSS/Update

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	DTLS DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
Test User Laptop	Tester's Laptop	SSH , DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark ( 4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Kali GNU-Linux Rolling 2023.3	Manually set and verified.	openssl (1.1f) OpenSSH_9.3p2
Management Workstation	Remote Access	SSH , DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6)
Console Switch	Console	NA	Linux Brain- Console (3.10.0-uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA

#### 4.2.3 DTLSC

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	DTLS DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
Test User Laptop	Tester's Laptop	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark ( 4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Ubuntu 20.04.6 LTS	Manually set and verified.	Openssl (1.1f ) TLS-Attacker (2.0) tcp- replay tool ( )
Management Workstation	Remote Access	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6)
Network Bridge	MITM Tool	DTLS	Ubuntu 22.04.3 LTS	Manually set and verified.	MITM tool(0.8.4)
Console Switch	Console	NA	Linux Brain- Console (3.10.0-uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA

#### 4.2.4 DTLSS/X509-Rev

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2	TOE	DTLS DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
Test User Laptop	Tester's Laptop	SSH , DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Ubuntu 20.04.6 LTS	Manually set and verified.	openssl (1.1f) TLS-Attacker (2.0) dtlss-byte-change v1.0
Test VM	Packet Capture	SSH	Ubuntu 20.04.6 LTS	Manually set and verified.	openssl (1.1f) TLS-Attacker (2.0) dtlss-byte-change v1.0
Management Workstation	Remote Access	SSH , DTLS	Windows 10 Pro -64-bit	Manually set and verified.	MITM tool (0.8.4)
Console Switch	Console	NA	Linux Brain- Console (3.10.0-uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA



#### 4.2.5 DTLS-MA

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
		DTLS			
Test User Laptop	Tester's Laptop	SSH , DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Ubuntu 20.04.6 LTS	Manually set and verified.	openssl (1.1f) TLS-Attacker (2.0)
Test VM	Packet Capture	SSH	Ubuntu 20.04.6 LTS	Manually set and verified.	openssl (1.1f) TLS-Attacker (2.0)
Management Workstation	Remote Access	SSH , DTLS	Windows 10 Pro -64-bit	Manually set and verified.	MITM tool (0.8.4)
Network Bridge	MITM Tool	DTLS	Ubuntu 22.04.3 LTS	Manually set and verified.	NA
Console Switch	Console	NA	Linux Brain- Console (3.10.0- uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA

#### 4.2.6 Firewall

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	FW	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
		FW			
Test User Laptop	Tester's Laptop	SSH	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (3.6.0 ) xca (2.1.1)
Test VM 1	Packet Capture	SSH	Kali GNU/Linux " 2023.3	Manually set and verified.	NA
Test VM 2	Packet Capture	SSH	Ubuntu 20.04.6 LTS	Manually set and verified.	NA
Management Workstation	Remote Access	SSH ,	Windows 10 Pro -64-bit	Manually set and verified.	MITM tool (0.8.4)
Console Switch	Console	NA	Linux Brain- Console (3.10.0- uc0)		
Switch	Lab Switch	NA	NA	NA	NA

#### 4.2.7 SSHC

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
		DTLS			
Test User Laptop	Tester's Laptop	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark ( 4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Kali GNU-Linux Rolling 2023.3	Manually set and verified.	openssl (1.1f) OpenSSH_9.3p2 Acumen-sshc tool v
Management Workstation	Remote Access	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6) xca (2.1.2)
Console Switch	Console	NA	Linux Brain-Console (3.10.0-uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA

#### 4.2.8 SSHS

Device Name	Function	Protocols	OS, including version	Time	Software & Tools, including version
TRX-R2 Voyager VMm Voyager VM3	TOE	DTLS	KlasOS keel v5.4.0rc7	Manually set and verified.	NA
		DTLS			
Test User Laptop	Tester's Laptop	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark ( 4.0.6 ) xca (2.1.2)
Test VM	Packet Capture	SSH	Kali GNU-Linux Rolling 2023.3	Manually set and verified.	openssl (1.1f) OpenSSH_9.3p2 Acumen-sshs tool v1.1.2
Management Workstation	Remote Access	SSH DTLS	Windows 10 Pro -64-bit	Manually set and verified.	Wireshark (4.0.6) xca (2.1.2)
Console Switch	Console	NA	Linux Brain-Console (3.10.0-uc0)	NA	NA
Switch	Lab Switch	NA	NA	NA	NA

### 4.3 Test Time and Location

All testing was conducted on the TRX, VM3 and VMM TOE models outlined in the Security Target. The final version of the TOE software running on the devices is KlasOS.keel.v5.4.0rc7.bin. Testing took place at the Acumen Security

offices located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from May 2023 through July 2024.

Regression testing was also conducted on the TOE due to new builds being provided throughout the course of testing to resolve issues. All regression testing took place at the same office mentioned above and would occur after every new build was provided to the lab from the vendor. The original version of the build was 5.4.0rc3 and the final version was 5.4.0rc7.

Regression testing was performed on the following test cases between receiving every build to ensure nothing was changed:

- FCS\_NTP\_EXT.1.1 Test #1
- FMT\_MTD.1/CryptoKeys Test #1
- FTA\_TAB.1 Test #1
- FCS\_DTLSS\_EXT.1.1 Test #1
- FFW\_RUL\_EXT.1 Test #1
- FCS\_SSHS\_EXT.1.2 Test #1
- FCS\_TLSS\_EXT.1.2 Test #1
- FIA\_X509\_EXT.1.1/Rev Test #5
- FPT\_TUD\_EXT.1 Test #1

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day that testing occurred, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

## 5 Detailed Test Cases (TSS and the AGD Activities)

### 5.1 Mandatory Requirements

#### 5.1.1 Security Audit (FAU)

##### 5.1.1.1 FAU\_GEN.1 Audit Data Generation

###### 5.1.1.1.1 FAU\_GEN.1 TSS

#### Objective:

- For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU\_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key.
- The evaluator shall ensure that the mapping of audit events to TOE components accounts for, and is consistent with, information provided in Table 1, as well as events in Tables 2, 4, and 5 (as applicable to the overall TOE). The evaluator confirmed that all components defined as generating audit information for a particular SFR contributed to that SFR as defined in the mapping of SFRs to TOE components, and that the audit records generated by each component covered all the SFRs that it implements.

#### Evaluator Findings:

- The evaluator reviewed the TSS and ensured that it identifies the relevant key based on what information is logged.  
The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_GEN.1' and 'FAU\_GEN.2'  
Upon investigation, the evaluator found that The TSS states that: **Administrative tasks of generating, importing and deleting cryptographic keys identify the keys unique name. SSH public keys are identified by the username in the logs on the TOE.**
- The evaluator reviewed the TSS and ensured that the mapping of audit events to TOE components accounts for, and is consistent with, information provided in Table 1, as well as events in Tables 2, 4, and 5 (as applicable to the overall TOE). The evaluator confirmed that all components defined as generating audit information for a particular SFR contributed to that SFR as defined in the mapping of SFRs to TOE components, and that the audit records generated by each component covered all the SFRs that it implements.  
The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_GEN.1' and 'FAU\_GEN.2'  
Upon investigation, the evaluator found that the TSS states that: **The TOE generates a comprehensive set of audit logs that identify specific TOE operation whenever an auditable event occurs. Auditable events are specified in Table 13 – Security Functional Requirements and Auditable Events (ST). Each of the events specified in the audit records is in enough detail to identify the user with which the event is associated, when the event occurred, where the event occurred, the outcome of the event and the type of event that occurred.**

#### Verdict:

PASS

5.1.1.1.2 FAU\_GEN.1 AGD

**Objective:**

- The evaluator shall check the AGD and ensure that it provides an example of each auditable event required by FAU\_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection-based SFR Sections as applicable, shall be provided from the actual audit record).
- The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes.
- The evaluator shall examine the AGD and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP.
- The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding AGD satisfies the requirements related to it.
- If the optional SFR FFW\_RUL\_EXT.2 is claimed by the TOE, the evaluator shall also check the guidance documentation to ensure that it describes the relevant audit record specified in Table 3 of the PP-Module.

**Evaluator Findings:**

- The evaluator checked the AGD and ensured that it provides an example of each auditable event required by FAU\_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection based SFR Sections as applicable, was provided from the actual audit record).

The relevant information is found in the following section(s): **8.2 ‘System Log’**

Upon investigation, the evaluator found that the AGD lists audit logs examples of each auditable event required by FAU\_GEN.1

- The evaluator examined the AGD Section 8.2 titled ‘**System Log**’ and made a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. Upon investigation, the evaluator found that **the following are applicable:**

<u>Administrative Activity</u>	<u>Method (Command) CLI Configuration</u>	<u>Section</u>
Start-up and shut-down of the audit functions;	<ul style="list-style-type: none"> <li>• logging audit local</li> <li>• no logging audit local</li> </ul>	<ul style="list-style-type: none"> <li>• ‘Starting and Stopping Local Audit Logging’</li> </ul>
Administrative login and logout	<ul style="list-style-type: none"> <li>• KlasOS login: klas Password:</li> <li>• Exit</li> </ul>	<ul style="list-style-type: none"> <li>• Administrator Authentication</li> <li>• User Identification and Authentication</li> <li>• Session Termination</li> </ul>
Changes to TSF data related to configuration changes	<ul style="list-style-type: none"> <li>• logging host XXXX</li> <li>• no logging host XXXX</li> </ul>	<ul style="list-style-type: none"> <li>• Sending Logs to Syslog Server</li> </ul>
Generating/import of, changing, or deleting of cryptographic keys	<ul style="list-style-type: none"> <li>• crypto key generate rsa general-keys modulus &lt;2048 3072 4096&gt; label &lt;label name</li> </ul>	<ul style="list-style-type: none"> <li>• Cryptographic Key Generation</li> </ul>

	<ul style="list-style-type: none"> <li>• crypto key zeroize &lt;rsa   ec&gt;</li> </ul>	<ul style="list-style-type: none"> <li>• Cryptographic Key Zeroization</li> </ul>
Resetting passwords	<ul style="list-style-type: none"> <li>• username &lt;username&gt; secret &lt;password&gt;</li> </ul>	<ul style="list-style-type: none"> <li>• Passwords</li> </ul>

- The evaluator performed this activity as part of the activities associated with ensuring that the corresponding AGD satisfies the requirements related to it.
- The optional SFR FFW\_RUL\_EXT.2 is not claimed by the TOE.

**Verdict:**

PASS.

5.1.1.2 FAU\_GEN.2 User Identity Association

5.1.1.2.1 TSS & AGD

The TSS and AGD requirements for FAU\_GEN.2 are already covered by the TSS and AGD requirements for FAU\_GEN.1.

5.1.1.3 FAU\_STG\_EXT.1 Protected Audit Event Storage

5.1.1.3.1 FAU\_STG\_EXT.1 TSS

**Objective:**

- The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
- The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
- The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally.
- The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally.
- The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.
- The evaluator shall examine the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE shall also be detailed in the TSS.
- The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in real- time or periodically. In case the TOE does not perform transmission in real- time the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.

## Evaluator Findings:

- The evaluator examined the TSS and ensured that it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided .
- The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_STG\_EXT.1'  
Upon investigation, the evaluator found that the TSS states that: **SSH is used to provide a trusted communication channel with the syslog server.**
- The evaluator examined the TSS and ensured it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.

The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_STG\_EXT.1'

Upon investigation, the evaluator found that the TSS states **that Data stored locally is kept in an audit log file. Each log file is rotated at approximately 10MB in size but due to the lag between the appending to the log and the rotation of the log, the size may grow larger than this. Each log will never grow larger than 20MB in size. The previous log is overwritten by the new log. Neither a TOE user nor a Security Administrator has system privileges to modify the audit records.**

- The evaluator examined the TSS and ensured that it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally.

**The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_STG\_EXT.1'  
Upon investigation, the evaluator found that the TSS states that:TOE is standalone and audit data is stored locally.**

- The evaluator examined the TSS and ensured that it details the behavior of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. Other actions' are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE is detailed in the TSS

The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_STG\_EXT.1'

Upon investigation, the evaluator found that the TSS states that:**Each log file is rotated at approximately 10MB in size but due to the lag between the appending to the log and the rotation of the log, the size may grow larger than this. Each log will never grow larger than 20MB in size. The previous log is overwritten by the new log.**

- The evaluator examined the TSS and ensured that it details whether the transmission of audit information to an external IT entity can be done in real- time or periodically. In case the TOE does not perform transmission in real- time the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.

The relevant information is found in the following section(s): TOE Summary Specification 'FAU\_STG\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **Audit events are stored locally and are also sent to an external audit server in real-time.**

## Verdict:

PASS.

### 5.1.1.3.2 FAU\_STG\_EXT.1 AGD

#### Objective:

- The evaluator shall also examine the AGD to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
- The evaluator shall also examine the AGD to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.
- The evaluator shall also ensure that the AGD describes all possible configuration options for FAU\_STG\_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.

#### Evaluator Findings:

- The evaluator examined the AGD and ensured it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server, as well as configuration of the TOE needed to communicate with the audit server.

The relevant information is found in the following section(s): **9 ‘SSH Tunnel for Trusted Channel’ ,9.3 ‘Configure SSH Tunnel’**

Upon investigation, the evaluator found that the AGD states that: **The TOE uses an SSH tunnel for the Trusted Channel for syslog messages that are sent from the TOE to a remote syslog server.**

**To configure the SSH tunnel on the TOE, run the following command in global configuration mode.**

- **ssh tunnel username <username> host <syslog server IP> localport 50514 remoteport 514**

**Replace <username> with the correct username on the syslog server we will be building the SSH tunnel to.**

**The <syslog server IP> is the IP address of the syslog server.**

**Localport can be any unused port on the TOE.**

**Remote port is the port the syslog server will be listening to for incoming syslog messages.**

- The evaluator also examined the AGD and determined that it describes the relationship between the local audit data and the audit data that are sent to the audit log server.

The relevant information is found in the following section(s):**8.Logging and Auditing**

Upon investigation, the evaluator found that the AGD states that:

- **Audit log:**
  - **This logs every CLI command entered by a user or administrator including:**
    - **Security related changes**
    - **Generating/import of modification or deletion of cryptographic keys**
    - **Resetting passwords**
    - **Starting and stopping services**
  - **The audit log cannot be stopped or disabled by an administrator. It is always on.**
- **System log:**
  - **Logs all general system and authentication messages including:**
    - **User and administrator authentication events for both local and remote sessions**



- Self-test firmware integrity pass/fail messages.
  - Clock modification notifications.
- The system log cannot be stopped or disabled by an administrator. It is always on.
- The evaluator ensured that the AGD describes all possible configuration options for FAU\_STG\_EXT.1.3 and the resulting behaviour of the TOE for each possible configuration. The description of possible configuration options and resulting behaviour corresponds to those described in the TSS.

The relevant information is found in the following section(s): **8. Logging and Auditing**

Upon investigation, the evaluator found that the AGD states that: **Each log file is rotated at approximately 10MB in size but due to the lag between the appending to the log and the rotation of the log, the size may grow larger than this. Each log will never grow larger than 20MB in size. This is not a configurable option. To check the name and current size of the log files, run the following command in Privileged EXEC mode.**

**Verdict:**

PASS.

**5.1.2 Cryptographic Support (FCS)**

**5.1.2.1 FCS\_CKM.1 Cryptographic Key Generation**

**5.1.2.1.1 FCS\_CKM.1 TSS**

**Objective:**

- The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
- If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

**Evaluator Findings:**

- The evaluator ensured that the TSS identifies the key sizes supported by the TOE. The ST specifies more than one scheme, the evaluator examined the TSS to verify that it identifies the usage for each scheme.

The relevant information is found in the following section(s): TOE Summary Specification ‘**FCS\_CKM.1**’

Upon investigation, the evaluator found that the TSS states that: **The TOE supports several cryptographic key generation schemes which include RSA 2048-bit, ECC P-256, ECC P-384, ECC P-521, and FFC safe-prime groups.**

Key Generation	SFR	Usage
RSA	FCS_DTLSC_EXT.1	DTLS server and DTLS client.
	FCS_DTLSC_EXT.2	
	FCS_DTLSS_EXT.1	HTTPS server
	FCS_DTLSS_EXT.2	
	FCS_TLSS_EXT.1	
Elliptic curve	FCS_SSHS_EXT.1	SSHs for administration and SSHC tunnel to syslog server
	FCS_SSHC_EXT.1	
FFC	FCS_SSHS_EXT.1	SSHs for administration and SSHC tunnel to syslog server
	FCS_SSHC_EXT.1	

**Verdict:**

PASS.



5.1.2.1.2 FCS\_CKM.1 AGD

**Objective:**

- The evaluator shall verify that the AGD instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.

**Evaluator Findings:**

- The evaluator verified that the AGD instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.

The relevant information is found in the following section(s): **‘Services, SSH Tunnel for Trusted Channel’, ‘SDWAN Encryption and encryption-mode’, ‘Introduction to Certificate Manager’**

Upon investigation, the evaluator found that the AGD states that:

**SSH client on the TOE is restricted to the following algorithms:**

- **Encryption using AES-CBC-256 or AES-CBC-128**
- **Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384**
- **Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512**
- **Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.**

**Verdict:**

PASS.

5.1.2.2 FCS\_CKM.2 Cryptographic Key Establishment

5.1.2.2.1 FCS\_CKM.2 TSS [TD0580]

**Objective:**

- The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS\_CKM.1.1.
- If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
- The intent of this activity is to be able to identify the scheme being used by each service. This would mean, for example, one way to document scheme usage could be as shown in the table. The information provided in the example above does not necessarily have to be included as a table but can be presented in other ways as long as the necessary data is available.

**Evaluator Findings:**

- The evaluator ensured that the supported key establishment schemes correspond to the key generation schemes identified in FCS\_CKM.1.1.

The relevant information is found in the following section(s): TOE Summary Specification **‘FCS\_CKM.2’**

Upon investigation, the evaluator found that the TSS states that: **In agreement with the key generation schemes the RSA-based, Elliptic curve-based, and Finite field-based key establishment schemes are supported as detailed in FCS\_CKM.2.**

- The evaluator ensured that the TSS Section titled **‘FCS\_CKM.2’** identifies the key establishment schemes supported by the TOE. The ST specifies more than one scheme, the evaluator examined the TSS to verify that it identifies the usage for each scheme. The TSS states the key establishment schemes in the below table:

Key Establishment	SFR	Usage
-------------------	-----	-------

Scheme		
RSA	FCS_DTLSS_EXT.1 FCS_DTLSC_EXT.2 FCS_DTLSS_EXT.1 FCS_DTLSS_EXT.2 FCS_TLSS_EXT.1	DTLS server and DTLS client. HTTPS server
Elliptic curve	FCS_SSHS_EXT.1 FCS_SSHC_EXT.1	SSHS for administration and SSHC tunnel to syslog server
FFC	FCS_SSHS_EXT.1 FCS_SSHC_EXT.1	SSHS for administration and SSHC tunnel to syslog server

**Verdict:**

PASS.

5.1.2.2.2 FCS\_CKM.2 AGD

**Objective:**

- The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).

**Evaluator Findings:**

- The evaluator verified that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).

The relevant information is found in the following section(s): titled ‘**Services, SSH Tunnel for Trusted Channel’, ‘SDWAN Encryption and encryption-mode’**

Upon investigation, the evaluator found that the AGD states :

The HTTPS server on the TOE only supports the following algorithms using an RSA key size of 2048, 3072 or 4096 bits:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288

SSH client on the ToE is restricted to the following algorithms:

- Encryption using AES-CBC-256 or AES-CBC-128
- Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384
- Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512
- Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.

**Verdict:**

PASS.

### 5.1.2.3 FCS\_CKM.4 Cryptographic Key Destruction

#### 5.1.2.3.1 FCS\_CKM.4 TSS

##### Objective:

- The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT\_APW.EXT.1 and FPT\_SKP\_EXT.1, are accounted for<sup>2</sup>). In particular, if a TOE claims not to store plaintext keys in non-volatile memory, then the evaluator checks that this is consistent with the operation of the TOE.
- The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs). Note that where selections involve ‘destruction of reference’ (for volatile memory) or ‘invocation of an interface’ (for non-volatile memory) then the relevant interface definition is examined by the evaluator to ensure that the interface supports the selection(s) and description in the TSS. In the case of non-volatile memory, the evaluator includes in their examination the relevant interface description for each media type on which plaintext keys are stored. The presence of OS-level and storage device-level swap and cache files is not examined in the current version of the Evaluation Activity.
- Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS\_CKM.4.
- The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation Section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
- Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.

##### Evaluator Findings:

- The evaluator examined the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. The evaluator confirmed that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT\_APW.EXT.1 and FPT\_SKP\_EXT.1, are accounted for). In particular, the evaluator checked that the claim not to store plaintext keys in non-volatile memory is consistent with the operation of the TOE.

The relevant information is found in the following section(s): TOE Summary Specification: ‘**FCS\_CKM.4**’

Upon investigation, the evaluator found that the TSS states that **The TOE stores plaintext keys in volatile and non-volatile storage. The TOE satisfies all requirements for destruction of keys and CSPs as specified in FCS\_CKM.4. Please refer to Table 19 – Key Storage and Zeroization of Security Target.**

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
EC Session Keys	Ephemeral Session Key for SSH Session Establishment	Ephemeral; stored in RAM (Volatile storage)	Overwritten with zeroes at end of session.
Diffie Hellman Group 14 Session Keys	Ephemeral Session Key for SSH Session Establishment	Ephemeral; stored in RAM (Volatile storage)	Overwritten with zeroes at end of session.
RSA Key	Signature Generation, Signature Verification for SSH public key authentication.	Restricted key partition in plaintext (Non-Volatile storage)	Deleted with read-verify when any of the designated cryptographic key zeroization commands identified in AGD are executed by the administrator.  Key zeroization will instruct a part of the TOE to destroy the abstraction that represents the key. Generating a new key will overwrite and erase any existing keys and replacing the old keys with a new key value.
		While in use, RSA keys are held in RAM (Volatile storage)	Overwritten with zeroes when the key is no longer in use (after performing a cryptographic operation) or overwritten with a new value of the key when a new key value.
ECDSA Key	Signature Generation. Signature Verification for SSH public key authentication and verification of trusted updates.	Restricted key partition in plaintext (Non-Volatile storage)	Deleted with read-verify when any of the designated cryptographic key zeroization commands identified in AGD are executed by the administrator.  Key zeroization will instruct a part of the TOE to destroy the abstraction that represents the key. Generating a new key will overwrite and erase any existing keys and replacing the old keys with a new key value.
		While in use, ECDSA keys	Overwritten with zeroes when the key is

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
		are held in RAM (Volatile storage)	no longer in use (after performing a cryptographic operation)
HMAC Key	Keyed Hashing for SSH	While in use, keys for HMAC keyed hashing are held in RAM (Volatile storage)	Overwritten with zeroes when the key is no longer in use (after performing a cryptographic operation).
AES Session Keys	SSH Data Encryption	Ephemeral; stored in RAM (Volatile storage)	Overwritten with zeroes at end of session

- The evaluator confirmed that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT\_APW.EXT.1 and FPT\_SKP\_EXT.1, are accounted for). In particular, the evaluator checked that the claim not to store plaintext keys in non-volatile memory is consistent with the operation of the TOE.

The relevant information is found in the following section(s): TOE Summary Specification : ‘FCS\_CKM.4’

Upon investigation, the evaluator found that the TSS states that **The TOE stores plaintext keys in volatile and non-volatile storage.**

- The evaluator checked to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).

The relevant information is found in the following section(s): TOE Summary Specification ‘FCS\_CKM.4’.

Upon investigation, the evaluator found that the details can be found in the **Table 18 – Key Storage and Zeroization of Security Target.**

- Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator checked that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS\_CKM.4.

The relevant information is found in the following section(s): TOE Summary Specification ‘FCS\_CKM.4’.

Upon investigation, the evaluator found that the TSS states that: The TOE stores plaintext keys only. Hence this Assurance activity is not applicable for this TOE.

- The evaluator checked that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below).

The relevant information is found in the following section(s): TOE Summary Specification ‘FCS\_CKM.4’.

Upon investigation, the evaluator further checked the guidance section 6.2 states that: There are no circumstances that may not strictly conform to the key destruction requirements or situations where key destruction may be delayed at the physical layer

- Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examined the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.

The relevant information is found in the following section(s): TOE Summary Specification ‘FCS\_CKM.4’.

Upon investigation, the evaluator found that:**The TOE does not use of a value that does not contain any CSP to overwrite keys, hence, not relevant**

**Verdict:**

**PASS.**

**5.1.2.3.2 FCS\_CKM.4 AGD**

**Objective:**

- A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used).
- The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer. For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-levelling and garbage collection. This may result in additional copies of the key that are logically inaccessible but persist physically. Where available, the TOE might then describe use of the TRIM command<sup>3</sup> and garbage collection to destroy these persistent copies upon their deletion (this would be explained in TSS and Operational Guidance).

**Evaluator Findings:**

- The evaluator checked that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used).

The relevant information is found in the following section(s): **6.2. Cryptographic Key Zeroization**

Upon investigation, the evaluator found that the AGD states that: **There are no circumstances that may not strictly conform to the key destruction requirements or situations where key destruction may be delayed at the physical layer**

- The evaluator checked that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.

The relevant information is found in the section **6.2. Cryptographic Key Zeroization.**

Upon investigation, the evaluator found that the AGD states that: **There are no configurations or circumstances that do not strictly conform to the key destruction requirements found in FCS\_CKM.4. There are also no situations where the key destruction may be delayed at the physical layer.**

The evaluator examined the AGD Section titled '**Cryptographic Key Zeroization and Cryptographic key Management**' **ensured that identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS**

Upon investigation, the evaluator found that the Each private key generated is stored on the system flash and each key can be zeroized securely as per Common Criteria requirements. To generate a new SSH host key, you need to firstly zeroize any existing keypairs. This can be done using either of the following methods:

- Zeroize the individual key stored in flash:
  - `crypto key zeroize <ec|rsa> <label name>`
- Zeroize all existing keys:
  - `crypto key zeroize`

**Verdict:**

**PASS.**

#### 5.1.2.4 FCS\_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

##### 5.1.2.4.1 FCS\_COP.1/DataEncryption TSS

**Objective:**

- The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.

**Evaluator Findings:**

- The evaluator examined the TSS to ensure it 'identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.

The relevant information is found in the following section(s): TOE Summary Specification '**FCS\_COP.1/DataEncryption**'

Upon investigation, the evaluator found that the TSS states that:

**The TOE supports AES encryption and decryption conforming to CBC & GCM as specified in ISO 18033-3 and ISO 10116. The AES key size supported is 128 and 256 bits and the AES mode supported is CBC & GCM..**

**Verdict:**

**PASS.**

##### 5.1.2.4.2 FCS\_COP.1/DataEncryption AGD

**Objective:**

- The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.

**Evaluator Findings:**

Upon investigation, the evaluator found that the AGD **Section 7 'Remote Administration Using SSH'** states that: **These algorithms are not configurable on the ToE by an administrator. The algorithm used will depend on the algorithms the SSH client is using and the type of key generated on the ToE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the ToE. The TOE does not require configuration for key size(s) and mode(s) for data encryption/decryption, since it is pre-configured and fixed.**

**Verdict:**

**PASS.**



## 5.1.2.5 FCS\_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

### 5.1.2.5.1 FCS\_COP.1/SigGen TSS

#### Objective:

- The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.

#### Evaluator Findings:

- The evaluator examined the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.

The relevant information is found in the following section(s): TOE Summary Specification : 'FCS\_COP.1/SigGen'

Upon investigation, the evaluator found that the TSS states that: **The TOE provides cryptographic signature generation and verification services in accordance with the following cryptographic algorithms:**

- **RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048, 3072, and 4096 bits] according to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1\_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.**
- **Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256, 384 or 512 bits] according to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4**

#### Verdict:

PASS.

### 5.1.2.5.2 FCS\_COP.1/SigGen AGD

#### Objective:

- The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.

#### Evaluator Findings:

- Upon investigation, the evaluator found that the AGD **Section 7 'Remote Administration Using SSH'** states that: **These algorithms are not configurable on the ToE by an administrator. The algorithm used will depend on the algorithms the SSH client is using and the type of key generated on the ToE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the ToE. The TOE does not require configuration for key size(s) and mode(s) for data encryption/decryption, since it is pre-configured and fixed.**

#### Verdict:

PASS.

### 5.1.2.6 FCS\_COP.1/Hash Cryptographic Operation (Hash Algorithm)

#### 5.1.2.6.1 FCS\_COP.1/Hash TSS

**Objective:**

- The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

**Evaluator Findings:**

- The evaluator checked that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

The relevant information is found in the following section(s): TOE Summary Specification ‘FCS\_COP.1/Hash’.

Upon investigation, the evaluator found that the TSS states that:

**SSH, SNMP, NTP, and HTTPS support cryptographic hashing using SHA-1, SHA-256, SHA-384, or SHA-512 with message digest sizes of 160, 256, 384, and 512 bits.**

**Verdict:**

PASS.

#### 5.1.2.6.2 FCS\_COP.1/Hash AGD

**Objective:**

- The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.

**Evaluator Findings:**

- Upon investigation, the evaluator found that **The TOE does not require configuration for hash sizes, since it is pre-configured and fixed, and these mechanisms cannot be modified.**

**Verdict:**

PASS.

### 5.1.2.7 FCS\_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

#### 5.1.2.7.1 FCS\_COP.1/KeyedHash TSS

**Objective:**

- The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

**Evaluator Findings:**

- The evaluator examined the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

The relevant information is found in the following section(s): TOE Summary Specification

**FCS\_COP.1/KeyedHash**

Upon investigation, the evaluator found that the TSS states that:

**SSH, SNMP, NTP, and HTTPS support cryptographic hashing using SHA-1, SHA-256, SHA-384, or SHA-512 with message digest sizes of 160, 256, 384, and 512 bits. The key length, hash function used, block size, and output MAC lengths are identified in the table below.**

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-1	512 bits	160 bits	160 bits

HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-384	1024 bits	384 bits	384 bits
HMAC-SHA-512	1024 bits	512 bits	512 bits

**Verdict:**

PASS.

5.1.2.7.2 FCS\_COP.1/KeyedHash AGD

**Objective:**

- The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.

**Evaluator Findings:**

- The evaluator verified that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.

The relevant information is found in the following section(s): **‘Remote Administration Using SSH and SSH Tunnel for Trusted Channel’**

Upon investigation, the evaluator found that the AGD states that: SSH client on the ToE is restricted to the following algorithms:

- Encryption using AES-CBC-256 or AES-CBC-128
- Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384
- Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512
- Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.

**NOTE:** These algorithms are not configurable on the ToE by an administrator. The algorithm used will depend on the algorithms the SSH client is using and the type of key generated on the ToE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the ToE. The TOE does not require configuration for key size(s) and mode(s) for data encryption/decryption, since it is pre-configured and fixed.

**Verdict:**

PASS.

5.1.2.8 FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

5.1.2.8.1 FCS\_RBG\_EXT.1 TSS

**Objective:**

- The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min- entropy contained in the combined seed value.

### Evaluator Findings:

- The evaluator examined the TSS and determined that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min- entropy contained in the combined seed value.

The relevant information is found in the following section(s): TOE Summary Specification : **FCS\_RBG\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE implements a DRBG in accordance with ISO/IEC 18031:2011 using a CTR DRBG with AES. The noise source is the Intel RDSEED CPU instruction and is seeded with a minimum of 256 bits of entropy. The expected min-entropy rate for the noise source is 0.902120 bits of entropy per bit of noise output.**

### Verdict:

**PASS.**

#### 5.1.2.8.2 FCS\_RBG\_EXT.1 AGD

### Objective:

- The evaluator shall confirm that the AGD contains appropriate instructions for configuring the RNG functionality.

### Evaluator Findings:

- The evaluator confirmed that the AGD contains appropriate instructions for configuring the RNG functionality.

The relevant information is found in the following section(s): **Section 2.6 'TOE CC Compliant Configuration '**

Upon investigation, the evaluator found that the AGD states that: **The ToE Random Number Generator does not need to be configured and is automatically functional when the ToE has completed boot up.**

### Verdict:

**PASS.**

#### 5.1.3 Identification and Authentication (FIA)

##### 5.1.3.1 FIA\_AFL.1 Authentication Failure Management

###### 5.1.3.1.1 FIA\_AFL.1 TSS

### Objective:

- The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.
- The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).

### Evaluator Findings:

- The evaluator examined the TSS and determined that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS also describes the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability. The relevant information is found in the following section(s): TOE Summary Specification '**FIA\_AFL.1**'

Upon investigation, the evaluator found that the TSS states that: **An administrator can configure the maximum number of failed attempts using the CLI interface. The configurable range is between 1 and 255. attempts. When a user account has sequentially failed authentication for the configured number of times, the account will be locked, until a local administrator manually unlocks the account. If the lockout attempts are set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct. All failed attempts and lockouts are tracked by the TOE audit logs.**

- The evaluator examined the TSS and confirmed that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).

The relevant information is found in the following section(s): TOE Summary Specification **FIA\_AFL.1:**

Upon investigation, the evaluator found that the TSS states that: **The TOE will always allow a user to authenticate using the local console port, even if the user account is locked. This behavior is not configurable.**

#### Verdict:

PASS.

#### 5.1.3.1.2 FIA\_AFL.1 AGD

#### Objective:

- The evaluator shall examine the AGD to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.
- The evaluator shall examine the AGD to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA\_AFL.1.

#### Evaluator Findings:

- The evaluator examined the AGD and ensured that instructions for configuring the number of successive unsuccessful authentication attempts are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified all must be described. The AGD states the evaluator verified that all actions and mechanism implemented by the secure protocols are described.

The relevant information is found in the following section(s): **3.4. Account Locking**

Upon investigation, the evaluator found that the AGD states that:

**commands used to configure a maximum number of authentication attempts by a user from global configuration mode:**

```
aaa authentication attempts max-fail <number of failures>
```

**The account can be unlocked by a local console administrator using this command from privileged exec mode:**

```
clear aaa remote user username <username>
```

**max-fail attempts number is for consecutive login attempts and is not affected by automatic SSH session termination after its default number of failures. For example, if the lockout failure number is set to 5 and SSH disconnects after 3 failed attempts, if the user then tries to SSH unsuccessfully 2 more times, then that user will be locked out.**

- The evaluator examined the AGD and confirmed that it describes, and identifies the importance of, any actions that are required and ensured that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA\_AFL.1.

The relevant information is found in the following section(s): **3.4. Account Locking**

Upon investigation, the evaluator found that the AGD activity states that: **The TOE can be configured so that a remote user will be locked out after a number of unsuccessful login attempts. The remote user will be locked out until a local administrator manually unlocks the account from a local console.**

NOTE: **The ToE will always allow a user to authenticate using the local console port, even if the user account is locked. This behavior is not configurable.**

**Verdict:**

PASS.

5.1.3.2 FIA\_PMG\_EXT.1 Password Management

5.1.3.2.1 FIA\_PMG\_EXT.1 TSS[TD0792]

**Objective:**

- The evaluator shall check that the TSS to lists the supported special character(s) for the composition of administrator passwords.
- The evaluator shall check the TSS to ensure that the minimum\_password\_length parameter is configurable by a Security Administrator.
- The evaluator shall check that the TSS lists the range of values supported for the minimum\_password\_length parameter. The listed range shall include the value of 15.

**Evaluator Findings:**

- The evaluator examined the TSS and determined that it contains the lists of the supported special character(s) for the composition of administrator passwords.

The relevant information is found in the following Section(s): TOE Summary Specification 'FIA\_PMG\_EXT.1.'

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper- and lower-case letters, numbers, and special characters that include these characters include the following: "!", "@", "#", "\$", "%", "^", "&", "\*", "(", ")", "~", "<", ">", ",", ".", "/", ":", ";", "\_", "+", "-", "=", "{", "}", "[", "]", "|".**

- The evaluator examined the TSS to and ensured that the minimum\_password\_length parameter is configurable by a Security Administrator.

The relevant information is found in the following section(s): TOE Summary Specification 'FIA\_PMG\_EXT.1.'

Upon investigation, the evaluator found that the TSS states that: **The minimum password length can be configured by the Administrator.**

- The evaluator examined the TSS and determined that the TSS lists the range of values supported for the minimum\_password\_length parameter. The listed range includes the value of 15.

The relevant information is found in the following section(s): TOE Summary Specification: 'FIA\_PMG\_EXT.1.'

Upon investigation, the evaluator found that the TSS states that: **The minimum password length can be configured by the Administrator and can range from 15 to 128 characters.**

**Verdict:**

PASS.

5.1.3.2.2 FIA\_PMG\_EXT.1 AGD

**Objective:**

- The evaluator shall examine the AGD to determine that it:
  - a) identifies the characters that may be used in passwords and provides the AGD to security administrators on the composition of strong passwords, and
  - b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.

**Evaluator Findings:**

- The evaluator examined the AGD Section and determined that it:
  - a) identifies the characters that used in passwords and provides the AGD to security administrators on the composition of strong passwords. ,and
  - b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.

The relevant information is found in the following section(s): 'Passwords'

Upon investigation, the evaluator found that the AGD activity states that: **The minimum requirement is for a 15 character password containing at least one lower case character, upper case character, digit, and special character from the set !#\$%&()\*+,-./[]^\_`{|}~=<>@;:. The minimum password length can be increased by an administrator to up to 128 characters. The “\” character is interpreted as an escape character and is silently stripped from the password if entered.**

**The password must be at least 15 characters and should use a combination of the characters specified above. The minimum password length of at least 15 characters should be set using the “security passwords min-length” command .**

**Verdict:**

PASS.

5.1.3.3 FIA\_UIA\_EXT.1 User Identification and Authentication

5.1.3.3.1 FIA\_UIA\_EXT.1 TSS

**Objective:**

- The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”.
- The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.



- For distributed TOEs the evaluator shall examine that the TSS details how Security Administrators are authenticated and identified by all TOE components. If not, all TOE components support authentication of Security Administrators according to FIA\_UIA\_EXT.1 and FIA\_UAU\_EXT.2, the TSS shall describe how the overall TOE functionality is split between TOE components including how it is ensured that no unauthorized access to any TOE component can occur.
- For distributed TOEs, the evaluator shall examine the TSS to determine that it describes for each TOE component which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration. For each TOE component that does not support authentication of Security Administrators according to FIA\_UIA\_EXT.1 and FIA\_UAU\_EXT.2 the TSS shall describe any unauthenticated services/services that are supported by the component.

#### Evaluator Findings:

- The evaluator examined the TSS and determined that it describes the logon process for each logon method (local, remote (SSH)) supported for the product. This description contains information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”. The relevant information is found in the following section(s): **TOE Summary Specification FIA\_UIA\_EXT.1.** Upon investigation, the evaluator found that the TSS states that: **Access to the TOE is facilitated through by directly connecting to the TOE through serial console or remotely connecting to the TOE through SSHv2. Every user that authenticates is first logged in with non-administrative privileges with limited viewing functionalities. The user may then authenticate as an administrator with additional credentials to gain access to modifying functionalities. For remote administration, the TOE supports public key authentication and password-based authentication. If the user uses public key-based authentication and it is successful, then the user is granted access to the TOE. If the user uses password-based authentication and they provide valid username and password, then user is granted access to the TOE. If the user enters invalid user credentials, they will not be granted access.**
- The evaluator examined the TSS and determined that it describes which actions are allowed before user identification and authentication. The description covers authentication and identification for local and remote TOE administration. The relevant information is found in the following section(s): **TOE Summary Specification FIA\_UIA\_EXT.1.** Upon investigation, the evaluator found that the TSS states that: **Regardless of the interface at which the administrator interacts, the TOE prompts the user for a credential. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated.**  
**The TOE displays a banner in accordance with FTA\_TAB.1 before a user can log into the device. The TOE responds to ICMP requests without prior authentication.**
- For distributed TOEs the evaluator shall examine that the TSS details how Security Administrators are authenticated and identified by all TOE components. If not, all TOE components support authentication of Security Administrators according to FIA\_UIA\_EXT.1 and FIA\_UAU\_EXT.2, the TSS shall describe how the overall TOE functionality is split between TOE components including how it is ensured that no unauthorized access to any TOE component can occur.  
**Upon investigation, the evaluator found that** The TOE is not a distributed TOE hence this assurance activity is not applicable.



- For distributed TOEs, the evaluator shall examine the TSS to determine that it describes for each TOE component which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration. For each TOE component that does not support authentication of Security Administrators according to FIA\_UIA\_EXT.1 and FIA\_UAU\_EXT.2 the TSS shall describe any unauthenticated services/services that are supported by the component.

**Upon investigation, the evaluator found that** The TOE is not a distributed TOE hence this assurance activity is not applicable.

**Verdict:**

**PASS.**

5.1.3.3.2 FIA\_UIA\_EXT.1 AGD

**Objective:**

- The evaluator shall examine the AGD to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the AGD provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the AGD provides sufficient instruction on limiting the allowed services.

**Evaluator Findings:**

- The evaluator examined the AGD and determined that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator ensured that the AGD provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator determined that the AGD provides sufficient instruction on limiting the allowed services.

The relevant information is found in the following section(s): **‘User Identification and Authentication’, ‘Remote Administration using SSH’**

Upon investigation, the evaluator found that the AGD states that **The TOE provides a password-based login mechanism. The TOE supports both local administrations using the local console port and remote administration using SSH. Authentication is performed by providing the username and password and all passwords are obscured during logon. Successful authentication will give the CLI prompt and a message saying authentication was successful. An unsuccessful authentication attempt will drop the user back to the login prompt and display a message saying that login failed.**

**Remote administration of the device is allowable using SSH. The TOE can be configured to use public-key authentication or password authentication. The default setting is to attempt public-key authentication first and if no SSH public-key is found it will fall back to password authentication.**

**The TOE can be configured so that a remote user will be locked out after a number of unsuccessful login attempts. The remote user will be locked out until a local administrator manually unlocks the account from a local console.**

**Verdict:**

**PASS.**

5.1.3.4 FIA\_UAU\_EXT.2 Password-based Authentication Mechanism

Evaluation Activities for this requirement are covered under those for FIA\_UIA\_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA\_UIA\_EXT.1.

### 5.1.3.5 FIA\_UAU.7 Protected Authentication Feedback

#### 5.1.3.5.1 FIA\_UAU.7 AGD

##### Objective:

- The evaluator shall examine the AGD to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.

##### Evaluator Findings:

- The evaluator examined the AGD and determined that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.

The relevant information is found in the following section of AGD 3. User Identification and Authentication

Upon investigation, the evaluator found that the AGD states: **no configuration is necessary for obscuring of authentication data.**

##### Verdict:

PASS.

### 5.1.4 Security Management (FMT)

#### 5.1.4.1 FMT\_MOF.1/ManualUpdate

##### 5.1.4.1.1 FMT\_MOF.1/ManualUpdate AGD

##### Objective:

- The evaluator shall examine the AGD to determine that any necessary steps to perform manual update are described. The AGD shall also provide warnings regarding functions that may cease to operate during the update (if applicable).

##### Evaluator Findings:

- The evaluator examined the AGD and determined that any necessary steps to perform manual update are described. The AGD also provides warnings regarding functions that may cease to operate during the update (if applicable).

The relevant information is found in the following section(s): **2.1 Software installation.**

Upon investigation, the evaluator found that the AGD states : **The steps to install the new firmware.**

- **Verify the signature on the firmware image:**
- **The uploaded firmware image must be verified to check that the digital signature is correct before proceeding any further.**

**Specify that this newly copied image is the image to be booted: Once this command is executed, the new image will now load when the system is rebooted. A log message will be generated in the audit log signifying that the firmware has been installed and Reboot the device. Also warning states to Ensure the firmware image name that you use is a different name to an image that is already installed. If you overwrite the previous image with the new image and it fails the digital signature verification, the image will be deleted. This will result in no valid image present on the TOE. If the TOE is then rebooted, it will not boot up as no valid image is present.**

##### Verdict:

PASS.

## 5.1.4.2 FMT\_MTD.1/CoreData Management of TSF Data

### 5.1.4.2.1 FMT\_MTD.1/CoreData TSS

#### Objective:

- The evaluator shall examine the TSS to determine that, for each administrative function identified in the AGD; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
- If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.

#### Evaluator Findings:

- The evaluator examined the TSS and determined that, for each administrative function identified in the AGD; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator also confirmed that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.

The relevant information is found in the following section(s): TOE Summary Specification 'FMT\_MTD.1/Core Data' Upon investigation, the evaluator found that The TSS States that: **Administrative users are required to login before being provided with access to any administrative functions. Non-security administrators are not allowed to modify any TOE functions. No interface is available to an unauthenticated user except the login prompt. Any commands used to modify, and TOE functions is not made available to non-administrative users and its attempt to use them will result in an invalid action error.**

- If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator examined the TSS and determined that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.

The relevant information is found in the following section(s): TOE Summary Specification 'FMT\_MTD.1/Core Data'

Upon investigation, the evaluator found that the TSS states that: **The ability to modify the TOE's trust store (modify, import, generate) X509 certificates is restricted to the security administrator.**

#### Verdict:

PASS.

### 5.1.4.2.2 FMT\_MTD.1/CoreData AGD

#### Objective:

- The evaluator shall review the AGD to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the c PP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.
- If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the AGD to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way.
- If the TOE supports loading of CA certificates, the evaluator shall review the AGD to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store.

- The evaluator shall also review the AGD to determine that it explains how to designate a CA certificate a trust anchor.

#### Evaluator Findings:

- The evaluator reviewed the AGD and determined that each of the TSF-data-manipulating functions implemented in response to the requirements of the c PP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.

The relevant information is found in the following section(s): **'TOE CC Compliant Configuration'**

Upon investigation, the evaluator found that the AGD states that: **To ensure the TOE is operating in a CC compliant configuration the following actions must be performed on the TOE after the CC firmware image has been loaded and verified. The configuration must be completed before the TOE is connected to any network.**

- If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator reviewed the AGD and determined that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way.

The relevant information is found in the following section(s): Introduction to Certificate Manager

Upon investigation, the evaluator found that the AGD states that: The Certificate Manager (certmgr) is a feature that allows a KlasOS device to create certificate signing requests, store and manage certificate files through 'certmgr trustpoint' objects. The feature can be used with SDWAN in 'pki-DTLS' encryption-mode and in 'ip http secure-server'.

- If the TOE supports loading of CA certificates, the evaluator shall review the AGD to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store.

The relevant information is found in the following section(s): **'Generating and Adding Certificates to a Certificate Manager'**

Upon investigation, the evaluator found that the AGD states that: **Certificate manager certificates may only be used in conjunction with SDWAN ('certmgr' setting). The certificate manager feature allows multiple SDWAN interfaces to use the same certificates configured by a single trustpoint, thus simplifying configuration. And The steps to create and apply certificate to a trustpoint are given in the AGD.**

- The evaluator also reviewed the AGD and determined that it explains how to designate a CA certificate a trust anchor.

The relevant information is found in the following section(s): **. Reference the device and CA certificate in the trustpoint**

Upon investigation, the evaluator found that the AGD states that: **The CA\_cert\_chain.pem file may contain multiple intermediate CA certificates, however the device\_cert.pem may only contain the certificate for the device.**

```
KlasOS# configure terminal
KlasOS(config)# certmgr trustpoint mytruspoint RSA
KlasOS(cert-tp-mytruspoint)# device-cert flash: device_cert.pem
KlasOS(cert-tp-mytruspoint)# ca-cert-chain flash: CA_cert_chain.pem
The trustpoint is now ready to be used with SDWAN.
```

#### Verdict:

PASS.

### 5.1.4.3 FMT\_SMF.1 Specification of Management Functions

#### 5.1.4.3.1 FMT\_SMF.1 TSS

##### Objective:

- The evaluator shall examine the TSS, the AGD and the TOE as observed during all other testing and shall confirm that the management functions specified in FMT\_SMF.1 are provided by the TOE.
- The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).
- The evaluator shall examine the TSS and the AGD to verify they both describe the local administrative interface.
- The evaluator shall ensure the AGD includes appropriate warnings for the administrator to ensure the interface is local.
- For distributed TOEs with the option 'ability to configure the interaction between TOE components' the evaluator shall examine that the ways to configure the interaction between TOE components is detailed in the TSS and the AGD.
- The evaluator shall check that the TOE behavior observed during testing of the configured SFRs is as described in the TSS and the AGD.

##### Evaluator Findings:

- The evaluator examined the TSS Section '**FMT\_SMF.1**, the AGD Section '**Security Management**' and the TOE as observed during all other testing and confirmed that the management functions specified in FMT\_SMF.1 are provided by the TOE.
- The evaluator confirmed that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The TSS States that:  
**The available management functions are listed below and these can be accessed via the SSH command line interface both locally and remotely. The local interface can be accessed via a serial port and is identified with "tty" in the audit record.**
  - **Ability to administer the TOE locally and remotely;**
  - **Ability to configure the access banner;**
  - **Ability to configure the session inactivity time before session termination or locking;**
  - **Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;**
  - **Ability to configure the authentication failure parameters for FIA\_AFL.1;**
    - [
      - o **Ability to start and stop services;**
      - o **Ability to modify the behaviour of the transmission of audit data to an external IT entity;**
      - o **Ability to manage the cryptographic keys;**
      - o **Ability to configure the cryptographic functionality;**
      - o **Ability to re-enable an Administrator account;**
      - o **Ability to set the time which is used for time-stamps;**
      - o **Ability to configure NTP;**
      - o **Ability to configure the reference identifier for the peer;**
      - o **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;**

- o Ability to import X.509v3 certificates to the TOE's trust store;
- o Ability to manage the trusted public keys database;

**No other capabilities].**

- The evaluator examined the TSS Section 'FMT\_SMF.1 and the AGD Section 4 'Security Management' to verify they both describe the local administrative interface.

Upon investigation, the evaluator found that the TSS states that: **The available management functions are listed in FMT\_SMF.1.1 and these can be accessed via the SSH command line interface both locally and remotely. The local interface can be accessed via a serial port and is identified with "tty" in the audit record.**

Upon investigation, the evaluator found that the AGD states that: **The available management functions that are listed above can be accessed via the SSH command line interface both locally and remotely. The local interface can be accessed via a serial port and is identified with "tty" in the audit record.**

- The evaluator ensured the AGD includes appropriate warnings for the administrator to ensure the interface is local.
- For distributed TOEs with the option 'ability to configure the interaction between TOE components' the evaluator shall examine that the ways to configure the interaction between TOE components is detailed in the TSS and the AGD.  
Upon investigation, the evaluator found that the TSS states that: **The TOE is not a distributed TOE hence this assurance activity is not applicable.**
- The evaluator checked that the TOE behaviour observed during testing of the configured SFRs is as described in the TSS.

**Verdict:**

**PASS.**

5.1.4.4 FMT\_SMR.2 Restrictions on Security Roles

5.1.4.4.1 FMT\_SMR.2 TSS

**Objective:**

- The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.

**Evaluator Findings:**

- The evaluator examined the TSS and determined that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.

The relevant information is found in the following section(s): TOE Summary Specification: 'FMT\_SMR.2'

Upon investigation, the evaluator found that The TSS states that: **The TOE supports a security administrator role. The security administrator can administer the TOE locally or remotely.**

**Verdict:**

**PASS.**

5.1.4.4.2 FMT\_SMR.2 AGD

**Objective:**

- The evaluator shall review the AGD to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.

### Evaluator Findings:

- The evaluator reviewed the AGD and ensured that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.

The relevant information is found in the following section(s): **User Identification and Authentication** and Section **Remote Administration Using SSH**

Upon investigation, the evaluator found that the AGD states that: The ToE supports both local administration using the local console port and remote administration using SSH.

### Verdict:

PASS.

## 5.1.5 Protection of Security Functions (FPT)

### 5.1.5.1 FPT\_SKP\_EXT.1 Protection of TSF Data (for reading of all pre- shared, symmetric and private keys)

#### 5.1.5.1.1 FPT\_SKP\_EXT.1 TSS

#### Objective:

- The evaluator shall examine the TSS to determine that it details how any pre- shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

#### Evaluator Findings:

- The evaluator examined the TSS and determined that it details how any pre- shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.  
The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_SKP\_EXT.1'
- Upon investigation, the evaluator found that the TSS states that: **TThe TOE stores all private symmetric and asymmetric keys in secure storage and is not accessible through an interface to administrators. Passwords are obscured from the user from local and remote CLI interfaces. The TOE stores all password authentication data in a secure directory that is not accessible to administrators. Private keys may be destroyed or replaced but cannot be read**

#### Verdict:

PASS.

### 5.1.5.2 FPT\_APW\_EXT.1 Protection of Administrator Passwords

#### 5.1.5.2.1 FPT\_APW\_EXT.1 TSS

#### Objective:

- The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.



## Evaluator Findings:

- The evaluator examined the TSS and determined that it details how any pre- shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.

The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_APW\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **The TOE stores all password authentication data in a secure directory that is not readily accessible to administrators. Passwords are obscured from the user from both local and remote CLI interfaces. The passwords are stored as SHA-512 hash and are not in plaintext.**

## Verdict:

PASS.

### 5.1.5.3 FPT\_TST\_EXT.1 TSF Testing

#### 5.1.5.3.1 FPT\_TST\_EXT.1 TSS

## Objective:

- The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used).
- The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.
- For distributed TOEs the evaluator shall examine the TSS to ensure that it details which TOE component performs which self-tests and when these self- tests are run.

## Evaluator Findings:

- The evaluator examined the TSS and ensured that it details the self-tests that are run by the TSF; this description includes an outline of what the tests are actually doing(e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" is used).

The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_TST\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **TOE executes the following self-tests when powered on:**

**Integrity check – The TOE performs an integrity check of the installed firmware by comparing the 4096-bit digital signature of the complete firmware image during bootup before any configuration is loaded and interfaces are enabled.**

**FIPS module self-tests in accordance with the OpenSSL 3.0.8 FIPS 140-2 Policy – The TOE performs FIPS self-tests to test the integrity of the operational environment when the cryptographic module is first initialized during boot-up. This includes KAT and PCT on all supported algorithms. If any cryptographic self-test fails, the TOE will complete the boot process with all cryptographic functions disabled.**

**The entropy noise source health tests are performed during bootup as part of the self-tests. They also are run continuously during system runtime.**

**Entropy health testing – If the entropy noise source health testing fails, the TOE immediately reboots and logs an audit message at the local console.**

- The evaluator ensured that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.



The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_TST\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **The TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, the TOE will enter an error state.**

- For distributed TOEs the evaluator shall examine the TSS to ensure that it details which TOE component performs which self-tests and when these self- tests are run.

Upon investigation, the evaluator found that the: **The TOE is not a distributed TOE hence this assurance activity is not applicable.**

**Verdict:**

**PASS.**

**5.1.5.3.2 FPT\_TST\_EXT.1 AGD**

**Objective:**

- The evaluator shall also ensure that the AGD describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
- For distributed TOEs the evaluator shall ensure that the AGD describes how to determine from an error message returned which TOE component has failed the self-test

**Evaluator Findings:**

- The evaluator also ensured that the AGD describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors correspond to those described in the TSS.

The relevant information is found in the following section(s): 'Self-Tests'

Upon investigation, the evaluator found that the AGD activity states that: **The TOE performs the following self-tests:**

- **Integrity check of the firmware image (during bootup)**
- **During system boot the TOE performs an integrity check of the installed firmware by comparing the RSA 4096 using SHA-256 digital signature of the firmware image. This happens before any configuration has been loaded or any interfaces are enabled. If signature verification fails, all SSH functionality is disabled and the messages will be sent to the system log.**
  - **FIPS module self-tests in accordance with the OpenSSL 3.0.8 FIPS 140-2 Policy (during bootup)**
  - **The TOE performs FIPS self-tests to test the integrity of the operational environment when the cryptographic module is first initialized during boot-up. This includes KAT and PCT on all supported algorithms. If any cryptographic self-test fails, the TOE will complete the boot process with all cryptographic functions disabled.**
  - **Entropy self-tests (continuous and during bootup)**
  - **The entropy noise source health tests are performed during bootup as part of the self-tests. They also are run continuously during system runtime. If any of the entropy health tests fail, the system will reboot immediately, and an error message will be displayed to the console.**
- **IMPORTANT: If any cryptographic algorithm known-answer tests or entropy self-tests failures are observed, the user should no longer use the device for cryptographic operations with the current firmware image. The user should try the following:**
  - 1.Load a new firmware image and check if the issue still occurs.**
  - 2. If the problem continues to exist, please discontinue usage of the device and contact Klas Telecom for assistance.**

**NOTE: The administrator must get a valid Klas firmware image (See Section 1.4.2) and install it as per Section 2.1 'Software Installation'.**

- For distributed TOEs the evaluator shall ensure that the guidance documentation describes how to determine from an error message returned which TOE component has failed the self-test.

Upon investigation, the evaluator found that **The TOE is not distributed hence this assurance activity is not applicable.**

**Verdict:**

**PASS.**

5.1.5.4 FPT\_TUD\_EXT.1 Trusted Update

5.1.5.4.1 FPT\_TUD\_EXT.1 TSS

**Objective:**

- The evaluator shall verify that the TSS describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active.
- The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software).
- The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism.
- The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
- If the options 'Support automatic checking for updates' or 'Support automatic updates' are chosen from the selection in FPT\_TUD\_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.
- For distributed TOEs, the evaluator shall examine the TSS to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component. Alternatively, this description can be provided in the AGD. In that case the evaluator should examine the AGD instead.
- If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT\_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.

**Evaluator Findings:**

- The evaluator verified that the TSS describes how to query the currently active version. The relevant information is found in the following section(s): TOE Summary Specification '**FPT\_TUD\_EXT.1**'

Upon investigation, the evaluator found that the TSS states that: **The Security Administrator can query the software version running on the TOE using the 'show version' command.**

- The evaluator verified that the TSS describes all TSF software update mechanisms for updating the system firmware and software.

The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_TUD\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **Before posting a new image for customer download, Klas creates a SHA256 hash of the image and then cryptographically digitally signs the hash using an RSA private key. This signed hash is then appended to the end of the firmware image. The public key is burned into the image already. The key that is burned into the image is used to validate the cryptographic signature of the update file. When software updates are made available by Klas, the Security Administrator can download and initiate installation of the update. The TOE will verify that the signed hash on the new image is valid before booting with the new image. If the image fails the signature check, then the image is deleted from the device and no upgrade occurs.**

- The evaluator verified that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS details this mechanism instead of the digital signature verification mechanism.

The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_TUD\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **The TOE will verify that the signed hash on the new image is valid before booting with the new image. If the image fails the signature check, then the image is deleted from the device and no upgrade occurs.**

- The evaluator verified that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.

The relevant information is found in the following section(s): TOE Summary Specification 'FPT\_TUD\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **TOE and is able to perform manual software updates. When software updates are made available by Klas, the Security Administrator can download and initiate installation of the update.**

- The evaluator verified that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.

Upon investigation, the evaluator found that the TOE does not select options 'support automatic checking for updates' or 'support automatic updates' selection in FPT\_TUD\_EXT.1.2.

- The evaluator examined the TSS and ensured that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component. Alternatively, this description can be provided in the AGD. In that case the evaluator should examine the AGD instead.

Upon investigation, the evaluator found that **The TOE is not distributed hence this assurance activity is not applicable.**

- The evaluator examined the TSS and ensured that, if a published hash is used to protect the trusted update mechanism, the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT\_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.

Upon investigation, the evaluator found that the TOE does not support use of published hash to protect the trusted update mechanism.

**Verdict:**

**PASS.**

**5.1.5.4.2 FPT\_TUD\_EXT.1 AGD**

**Objective:**

- The evaluator shall verify that the AGD describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the AGD needs to describe how to query the loaded but inactive version.
- The evaluator shall verify that the AGD describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
- If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the AGD describes how the Security Administrator can obtain authentic published hash values for the updates.
- For distributed TOEs the evaluator shall verify that the AGD describes how the versions of individual TOE components are determined for FPT\_TUD\_EXT.1, how all TOE components are updated, and the error conditions that may arise from checking or applying the update (e.g. failure of signature verification, or exceeding available storage space) along with appropriate recovery actions. . The AGD only has to describe the procedures relevant for the Security Administrator; it does not need to give information about the internal communication that takes place when applying updates.
- If this was information was not provided in the TSS: For distributed TOEs, the evaluator shall examine the AGD to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component.

**Evaluator Findings:**

- The evaluator verified that the AGD describes how to query the currently active version.  
The relevant information is found in the following section(s): **2.2 Verifying the Firmware Image**  
Upon investigation, the evaluator found that the AGD activity states that: **The administrator must verify after bootup that they are currently running the Common Criteria validated image. This is done by entering the ‘show version’ command in the CLI.**
- The evaluator verified that the AGD describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description includes the procedures for successful and unsuccessful verification. The description corresponds to the description in the TSS.  
The relevant information is found in the following section(s): **2.1 Software Installation**
- If a published hash is used to protect the trusted update mechanism, the evaluator verified that the AGD describes how the Security Administrator can obtain authentic published hash values for the updates.  
Upon investigation, the evaluator found that the AGD activity states that: **TOE does not use published Hash to protect trusted updates mechanism.**
- The evaluator examined the AGD and ensured that it describes how the versions of individual TOE components are determined for FPT\_TUD\_EXT.1, how all TOE components are updated, and the error conditions that may

arise from checking or applying the update (e.g. failure of signature verification or exceeding available storage space) along with appropriate recovery actions.

- Upon investigation, the evaluator found that **The TOE is not distributed hence this assurance activity is not applicable.**
- For distributed TOEs, the evaluator examined the AGD and ensured that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component.
- Upon investigation, the evaluator found that **The TOE is not distributed hence this assurance activity is not applicable.**

**Verdict:**

PASS.

5.1.5.5 FPT\_STM\_EXT.1 Reliable Time Stamps

5.1.5.5.1 FPT\_STM\_EXT.1 TSS[TD0632]

**Objective:**

- The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.
- If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.

**Evaluator Findings:**

- The evaluator examined the TSS and ensured that it lists each security function that makes use of time and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.

The relevant information is found in the following Section(s): TOE Summary Specification **FPT\_STM\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware. This clock is kept accurate and reliable using NTP. The following security functions make use of the system time:**

- **Audit events.**
- **Session inactivity**
- **SSH Rekey**

**The time can be manually updated by a Security Administrator.**

- The evaluator examined the TSS and found that the **TOE is not virtualized.**

**Verdict:**

PASS.

#### 5.1.5.5.2 FPT\_STM\_EXT.1 AGD[TD0632]

##### Objective:

- The evaluator examines the AGD to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the AGD instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.
- If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the AGD specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the AGD. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the AGD informs the administrator of the maximum possible delay.

##### Evaluator Findings:

- The evaluator examined the AGD and ensured that it instructs the administrator how to set the time. The AGD instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.

The relevant information is found in the following section(s): **Section 5.4 Time, 4.1 Services and 17. Configuring NTP.**

Upon investigation, the evaluator found that the AGD states that: **The TOE has a real-time clock that can be used as a reliable time source.**

- **The system clock can be set using the following command from Privileged EXEC mode:**

**clock set <HH:MM:SS> <MONTH> <DAY> <YEAR>**

**Modification of the system time is logged to the system log.**

**The format of the log message for manually changing the clock is as follows:**

**[Date and Time] [Hostname or IP address of TOE] [%SYS-6-CLOCKUPDATE]: [log message including old and new time] user <username> at <Source IP address**

- **NTP Client**

**Configure an NTP client in KlasOS with the following command in CONFIGURATION MODE**

- **KlasOS(conf)# ntp server <IP address>**
- **IP address is the IP address of the NTP server.**

**Client Authentication Key**

**If the NTP server supports cryptographic authentication using SHA-1, configure the correct key in KlasOS by appending a [key] option at the end of the ntp server command. In CONFIGURATION MODE:**

- **KlasOS(conf)# ntp authenticate**
- **KlasOS(conf)# ntp authentication-key 1 sha1 <shared secret>**
- **KlasOS(conf)# ntp trusted-key 1**
- **KlasOS(conf)# ntp server <IP address> key 1**

- The TOE does not support obtaining time from the underlying VS, this assurance activity is not applicable.

##### Verdict:

**PASS.**

## 5.1.6 TOE Access (FTA)

### 5.1.6.1 FTA\_SSL\_EXT.1 TSF-Initiated Session Locking

#### 5.1.6.1.1 FTA\_SSL\_EXT.1 TSS

##### Objective:

- The evaluator shall examine the TSS to determine whether local administrative session locking, or termination is supported and the related inactivity time period settings.

##### Evaluator Findings:

- The evaluator examined the TSS and determined that it details whether local administrative session locking or termination is supported and the related inactivity time period settings.

The relevant information is found in the following Section(s): TOE Summary Specification **FTA\_SSL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE, local CLI, and remote SSH interfaces. The configuration of inactivity periods is applied on a per-interface basis and can be applied to both local, and remote sessions in the same manner. When the interface has been idle for more than the configured period of time, the session will be terminated and will require reauthentication to establish a new session.**

##### Verdict:

PASS.

#### 5.1.6.1.2 FTA\_SSL\_EXT.1 AGD

##### Objective:

- The evaluator shall confirm that the AGD states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period.

##### Evaluator Findings:

- The evaluator confirmed that the AGD Section '**Session Termination**' states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period.

The relevant information is found in the following Section(s): **Section 3.3 Session Termination**

Upon investigation, the evaluator found that the TSS states that:

**A session inactivity timer can also be configured for both local console and remote SSH sessions. After this time period expires, the session will close and the user will be logged out.**

**To configure the session inactivity timer for the local console, do the following from Global Configuration mode:**

- **line console 0**
  - **exec-timeout <mins> <secs>**

**A log message similar to the following will be displayed in the system log when the user is automatically logged out of the console session.**

**To configure the session inactivity timer for a remote SSH session, do the following from Global configuration mode:**

- **line vty 0 4**
  - **exec-timeout <mins> <secs>**



A log message similar to the following will be displayed in the system log when the user is automatically logged out of the SSH session.

**Verdict:**

PASS.

5.1.6.2 FTA\_SSL.3 TSF-Initiated Termination

5.1.6.2.1 FTA\_SSL.3 TSS

**Objective:**

- The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.

**Evaluator Findings:**

- The evaluator examined the TSS Section '**FTA\_SSL.3**' and determined that it details the administrative remote session termination and the related inactivity time period.

The relevant information is found in the following Section(s): TOE Summary Specification **FTA\_SSL.3**

Upon investigation, the evaluator found that the TSS states that: **A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE, local CLI, and remote SSH interfaces. The configuration of inactivity periods is applied on a per-interface basis and can be applied to both, local, and remote sessions in the same manner. When the interface has been idle for more than the configured period of time, the session will be terminated and will require reauthentication to establish a new session.**

**Verdict:**

PASS.

5.1.6.2.2 FTA\_SSL.3 AGD

**Objective:**

- The evaluator shall confirm that the AGD includes instructions for configuring the inactivity time period for remote administrative session termination.

**Evaluator Findings:**

- The evaluator confirmed that the AGD Section '**Session Termination**' includes instructions for configuring the inactivity time period for remote administrative session termination.

The relevant information is found in the following Section(s): **Section 3.3 Session Termination**

Upon investigation, the evaluator found that the AGD activity states that: **A user can terminate their own interactive session by entering the 'exit' command at the CLI prompt.**

**If the user is in Privileged EXEC mode and the exit command is entered, the administrator session will end, and the user will be dropped back into User EXEC (non-administrator) mode. The user will need to enter the 'enable' command and re-authenticate to return to the Privileged EXEC mode.**

**If the user is in User EXEC mode and the exit command is entered the user will be logged out completely and will have to enter the username and password to log back in.**

**A session inactivity timer can also be configured for both local console and remote SSH sessions. After this time-period expires, the session will close, and the user will be logged out.**

**To configure the session inactivity timer for the local console, do the following from Global Configuration mode:**

- line console 0



- `exec-timeout <mins> <secs>`

A log message similar to the following will be displayed in the system log when the user is automatically logged out of the console session.

To configure the session inactivity timer for a remote SSH session, do the following from Global configuration mode:

- `line vty 0 4`
  - `exec-timeout <mins> <secs>`

A log message similar to the following will be displayed in the system log when the user is automatically logged out of the SSH session.

**Verdict:**

PASS.

5.1.6.3 FTA\_SSL.4 User-Initiated Termination

5.1.6.3.1 FTA\_SSL.4 TSS

**Objective:**

- The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.

**Evaluator Findings:**

- The evaluator examined the TSS Section '**FTA\_SSL.4**' and determined that it details how the local and remote administrative sessions are terminated.

The relevant information is found in the following Section(s): TOE Summary Specification **FTA\_SSL.4**

Upon investigation, the evaluator found that the TSS states that: **A Security Administrator is able to exit out of both local, and remote administrative sessions. For both local and remote sessions, the session is terminated by entering the "exit" command.**

**Verdict:**

PASS.

5.1.6.3.2 FTA\_SSL.4 AGD

**Objective:**

- The evaluator shall confirm that the AGD states how to terminate a local or remote interactive session.

**Evaluator Findings:**

- The evaluator confirmed that the AGD states how to terminate a local or remote interactive session.

The relevant information is found in the following Section(s): **Section 3.3 Session Termination**

Upon investigation, the evaluator found that the AGD activity states that: **A user can terminate their own interactive session by entering the 'exit' command at the CLI prompt.**

**If the user is in Privileged EXEC mode and the exit command is entered, the administrator session will end, and the user will be dropped back into User EXEC (non-administrator) mode. The user will need to enter the 'enable' command and re-authenticate to return to the Privileged EXEC mode.**

**If the user is in User EXEC mode and the exit command is entered the user will be logged out completely and will have to enter the username and password to log back in.**

**Verdict:**

PASS.

5.1.6.4 FTA\_TAB.1 Default TOE Access Banners

5.1.6.4.1 FTA\_TAB.1 TSS

**Objective:**

- The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS).
- The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).

**Evaluator Findings:**

- The evaluator checked the TSS and ensured that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS).  
The relevant information is found in the following section(s): TOE Summary Specification '**FTA\_TAB.1**'  
Upon investigation, the evaluator found that the TSS states that: **Access to the TOE is facilitated by directly connecting to the TOE through serial console or remotely connecting to the TOE through SSHv2.**
- The evaluator checked the TSS and ensured that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access.  
The relevant information is found in the following section(s): TOE Summary Specification '**FTA\_TAB.1**'  
Upon investigation, the evaluator found that the TSS states that: **Security Administrators can define a customized login banner that will be displayed at the local CLI and remote CLI (SSH). This banner will be displayed prior to allowing Security Administrators access.**

**Verdict:**

PASS.

5.1.6.4.2 FTA\_TAB.1 AGD

**Objective:**

- The evaluator shall check the AGD to ensure that it describes how to configure the banner message.

**Evaluator Findings:**

- The evaluator examined the AGD and ensured that it describes how to configure the banner message.  
The relevant information is found in the AGD Section(s) **3.2 Access Banner**  
Upon investigation, the evaluator found that the AGD states that: **The TOE can use the login banner to display an advisory notice and consent warning message regarding use of the TOE. This message is displayed before the login prompt is shown. To set the login banner do the following from Global Configuration mode:**
  - **Below command is used to set the login banner to "This is my login banner":**
    - **banner login "This is my login banner"****Also to add a banner with multiple lines, use "///" in the command above to add a carriage return/line feed (CR/LF).**
  - **Below command would set a multi-line login banner:**

- **banner login** *“This is my login banner///This is the second line of my login banner”*

**Verdict:**

**PASS.**

5.1.7 Trusted Path (FTP)

5.1.7.1 FTP\_ITC.1 Inter-TSF Trusted Channel

5.1.7.1.1 FTP\_ITC.1 TSS

**Objective:**

- The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint.
- The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.

**Evaluator Findings:**

- The evaluator examined the TSS and determined that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint.  
 The relevant information is found in the following Section(s): TOE Summary Specification **FTP\_ITC.1**  
 Upon investigation, the evaluator found that the TSS states that: **A remote audit server can be configured and the communication between the TOE and the audit server is protected by SSHv2 tunnel using public-key based authentication.**  
**The TOE acts as a client in the syslog connection. One or more TOEs may be connected in a SD-WAN and these connections are protected by DTLS. Though TSF data is not transmitted between TOEs, this SD-WAN connection could be used to administer another TOE. In this case the administrator session would be protected by the DTLS SD-WAN connection and SSH. The TOE can act as both a client and server in the SD-WAN connections.**
- The evaluator also confirmed that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.  
 The relevant information is found in the following section(s): TOE Summary Specification **FCS\_CKM.1 and FCS\_CKM.2**  
 Upon investigation, the evaluator found that the TSS states that: **All cryptographic information that pertains to syslog connections can be found under FCS\_SSHC\_EXT.1. All cryptographic information that pertains to SD-WAN connections can be found under FCS\_DTLSS\_EXT.1, FCS\_DTLSS\_EXT.2, FCS\_DTLSC\_EXT.1 and FCS\_DTLSC\_EXT.2.**
- **The TOE supports several cryptographic key generation schemes which include RSA 2048-bit, ECC P-256, ECC P-384, ECC P-521, FFC 2048-bit, and FFC safe-prime groups. These are detailed in FCS\_CKM.1.**

Key Generation	SFR	Usage
----------------	-----	-------

RSA	FCS_DTLCS_EXT.1 FCS_DTLSC_EXT.2 FCS_DTLSS_EXT.1 FCS_DTLSS_EXT.2 FCS_TLSS_EXT.1	DTLS server and DTLS client. HTTPS server
Elliptic curve	FCS_SSHS_EXT.1 FCS_SSHC_EXT.1	SSHS for administration and SSHC tunnel to syslog server
FFC	FCS_SSHS_EXT.1 FCS_SSHC_EXT.1	SSHS for administration and SSHC tunnel to syslog server

- In agreement with the key generation schemes the RSA-based, Elliptic curve-based, and Finite field-based key establishment schemes are supported as detailed in FCS\_CKM.2.

Key Establishment Scheme	SFR	Usage
RSA	FCS_DTLSC_EXT.1 FCS_DTLSC_EXT.2 FCS_DTLSS_EXT.1 FCS_DTLSS_EXT.2 FCS_TLSS_EXT.1	DTLS server and DTLS client. HTTPS server
Elliptic curve	FCS_SSHS_EXT.1 FCS_SSHC_EXT.1	SSHS for administration and SSHC tunnel to syslog server
FFC	FCS_SSHS_EXT.1 FCS_SSHC_EXT.1	SSHS for administration and SSHC tunnel to syslog server

**Verdict:**

PASS.

5.1.7.1.2 FTP\_ITC.1 AGD

**Objective:**

- The evaluator shall confirm that the AGD contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

**Evaluator Findings:**

- The evaluator confirmed that the AGD contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

The relevant information is found in the following Section(s): **Section 9 SSH Tunnel for Trusted Channel, Section 8.4 Sending Logs to Syslog Server, Section 8.1.1 Starting and Stopping Local Audit Logging, Section 10. Introduction to Certificate Manager and Section 11 SDWAN Encryption and encryption-mode**  
Upon investigation, the evaluator found that the AGD states that:

**The TOE uses an SSH tunnel for the Trusted Channel for syslog messages that are sent from the TOE to a remote syslog server.**

**To configure the SSH tunnel on the TOE, run the following command in global configuration mode.**

- `ssh tunnel username <username> host <syslog server IP> localport 50514 remoteport 514`

Replace <username> with the correct username on the syslog server we will be building the SSH tunnel to.  
The <syslog server IP> is the IP address of the syslog server.

Local port can be any unused port on the TOE

Remote port is the port the syslog server will be listening to for incoming syslog messages.

Initiation of the SSH tunnel is logged to the audit log. Section 8 'Logging and Auditing' for information on the audit log and the format of the log messages. The log message for initiating the SSH tunnel would look similar to the following:

The TOE allows the administrator to specify a syslog server to which all relevant logs can be sent.

On configuration of a remote syslog server, all contents of the System log and Audit log will be sent to the syslog server.

To configure the logs to be sent to a syslog server, use the following command in global configuration mode:

- `logging host 127.0.0.1`

**IMPORTANT NOTE:** All contents of the Audit log and System log are simultaneously sent to both the local logs on the TOE and the audit/syslog server.

The SSH tunnel will attempt to reconnect automatically when it detects the connection to the remote SSH server is broken. An administrator can also manually restart the tunnel by performing the following commands in global configuration mode:

- `no ssh tunnel username <username> host <syslog server IP> localport 50514 remoteport 514`
- `ssh tunnel username <username> host <syslog server IP> localport 50514 remoteport 514`

Replace <username> with the correct username on the syslog server we will be building the SSH tunnel to.  
The <syslog server IP> is the IP address of the syslog server.

Localport can be any unused port on the ToE

Remote port is the port the syslog server will be listening to for incoming syslog messages

For DTLS: A note in Sub section 11.1.1 "encryption-mode pki-DTLS" states that- If a DTLS connection is broken on the TOE, the TOE will reattempt the connection automatically. An administrator can also attempt to reconnect to the DTLS server from the TOE using the steps found in Section 11.

**Verdict:**

**PASS.**

5.1.7.2 FTP\_TRP.1/Admin Trusted Path

5.1.7.2.1 FTP\_TRP.1/Admin TSS

**Objective:**

- The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected.
- The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

**Evaluator Findings:**

- The evaluator examined the TSS and determined that the methods of remote TOE administration are indicated, along with how those communications are protected.

The relevant information is found in the following Section(s): TOE Summary Specification 'FTP\_TRP.1/Admin'  
Upon investigation, the evaluator found that the TSS states that: **Remote administration is performed using a CLI interface that is protected by SSHv2 using AES encryption. . .**

- The evaluator also confirmed that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement and are included in the requirements in the ST.

The relevant information is found in the following section(s): TOE Summary Specification 'FTP\_TRP.1/Admin and FCS\_SSHS\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **All requirements that secure this connection can be found in FCS\_SSHS\_EXT.1**

**Verdict:**

PASS.

5.1.7.2.2 FTP\_TRP.1/Admin AGD

**Objective:**

- The evaluator shall confirm that the AGD contains instructions for establishing the remote administrative sessions for each supported method.

**Evaluator Findings:**

- The evaluator confirmed that the AGD Section 'SSH Tunnel for Trusted Channel', 'Services' contains instructions for establishing the remote administrative sessions for each supported method.

The relevant information is found in the following Section(s): **Section 9. SSH Tunnel for Trusted Channel and 4.1 Services**

Upon investigation, the evaluator found that the AGD states that:

- **The TOE uses an SSH tunnel for the Trusted Channel for syslog messages that are sent from the TOE to a remote syslog server.**

**To configure the SSH tunnel on the TOE, run the following command in global configuration mode.**

**ssh tunnel username <username> host <syslog server IP> localport 50514 remoteport 514**

**Replace <username> with the correct username on the syslog server we will be building the SSH tunnel to.**

**The <syslog server IP> is the IP address of the syslog server.**

**Localport can be any unused port on the TOE**

**Remote port is the port the syslog server will be listening to for incoming syslog messages.**

**Initiation of the SSH tunnel is logged to the audit log. Section 8 'Logging and Auditing' for information on the audit log and the format of the log messages. The log message for initiating the SSH tunnel would look similar to the following:**

**2023-11-03T17:14:58.203957+00:00 VM3.0 sshd[29242]: Accepted password for acumensec from 10.1.3.169 port 53252 ssh2**

**2023-11-03T17:14:58.308931+00:00 VM3.0 CLI[29265]: (acumensec) (10.1.3.169) startup : Success**

**Verdict:**

PASS.

## 5.1.8 User Data Protection (FDP)

### 5.1.8.1 FDP\_RIP.2 Full Residual Information Protection

#### 5.1.8.1.1 FDP\_RIP.2 Full Residual Information Protection TSS

##### Objective:

- “Resources” in the context of this requirement are network packets being sent through (as opposed to “to”, as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet.
- The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets.
- The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.

##### Evaluator Findings:

- The evaluator reviewed the TSS Section ‘FDP\_RIP.2’ to ensure that it describes packet processing to the extent that they can determine that no data will be reused when processing network packets.
- The evaluator reviewed the TSS Section ‘FDP\_RIP.2’ to ensure that it describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.

The relevant information is found in the following Section(s): TOE Summary Specification FDP\_RIP.2

Upon investigation, the evaluator found that the TSS states that: **The TOE ensures that information from previous packets is never transmitted through the TOE. When a packet’s memory structure is initially created it is filled with zeroes to ensure that no residual information can be transmitted. Packets that are not the required length are padded with zeroes as required before the information is transmitted.**

##### Verdict:

PASS.

## 5.1.9 Firewall (FFW)

### 5.1.9.1 FFW\_RUL\_EXT.1 Stateful Traffic Filtering TSS

##### Objective:

- The evaluator shall verify that the TSS provides a description of the TOE’s initialization/startup process, which clearly indicates where processing of network packets begins to take place and provides a discussion that supports the assertion that packets cannot flow during this process.
- The evaluator shall verify that the TSS also include a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describe the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.
- The description shall also include a description how the TOE behaves in the situation where the traffic exceeds the amount of traffic the TOE can handle and how it is ensured that also in this condition stateful traffic filtering rules are still applied so that traffic does not pass that shouldn't pass according to the specified rules.

### Evaluator Findings:

- The evaluator reviewed the TSS Section 'FFW\_RUL\_EXT.1' to ensure that it provides a description of the TOE's initialization/startup process, which clearly indicates where processing of network packets begins to take place and provides a discussion that supports the assertion that packets cannot flow during this process.
- The evaluator reviewed the TSS Section 'FFW\_RUL\_EXT.1' to ensure that it includes a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describe the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.
- The evaluator reviewed the TSS Section 'FFW\_RUL\_EXT.1' to ensure that it includes a description how the TOE behaves in the situation where the traffic exceeds the amount of traffic the TOE can handle and how it is ensured that also in this condition stateful traffic filtering rules are still applied so that traffic does not pass that shouldn't pass according to the specified rules.

The relevant information is found in the following Section(s): TOE Summary Specification FFW\_RUL\_EXT.1

Upon investigation, the evaluator found that the TSS states that: **When the TOE first boots up, all network interfaces are in a shutdown state until the ACL configuration is processed and loaded. Once the ACL configurations are applied to every interface, then interfaces are enabled and will start processing inbound and outbound packet traffic. This prevents packets from bypassing ACLs during the boot-up process stateful traffic filtering is provided for ICMPv4, ICMPv6, IPv4, IPv6, TCP, and UDP network traffic by the traffic filtering service.**

The TOE administrator can define rules to permit or drop traffic based on the following parameters:

- ICMPv4 Type, Code
- ICMPv6: Type, Code
- IPv4: Source address, Destination Address, Transport Layer Protocol
- IPv6: Source address, Destination Address, Transport Layer Protocol
- TCP: Source Port, Destination Port, UDP, Source Port, Destination Port
- TOE network interface.

The administrator can define whether packets processed by the rules are logged.

Whenever packet traffic exceeds the maximum rate the TOE can handle, the TOE drops the excess traffic. This ensures that traffic which cannot be processed but does not match firewall filter rules will not be passed through.

### Verdict:

PASS.

#### 5.1.9.2 FFW\_RUL\_EXT.1 Stateful Traffic Filtering AGD

### Objective:

- The guidance documentation associated with this requirement is assessed in the subsequent test evaluation activities.

### Evaluator Findings:

- The evaluator checked the AGD Section 13.2 'Extended Access lists' and ensured that it is assessed in the subsequent test evaluation activities.

### Verdict:

PASS.





### 5.1.9.3 FFW\_RUL\_EXT.1.2/FFW\_RUL\_EXT.1.3/FFW\_RUL\_EXT.1.4 TSS

#### Objective:

- The evaluator shall verify that the TSS describes a stateful packet filtering policy, and the following attributes are identified as being configurable within stateful traffic filtering rules for the associated protocols:
  - ICMPv4
    - Type
    - Code
  - ICMPv6
    - Type
    - Code
  - IPv4
    - Source address
    - Destination Address
    - Transport Layer Protocol
  - IPv6
    - Source address
    - Destination Address
    - Transport Layer Protocol and where defined by the ST author, Extension Header Type, Extension Header Fields
  - TCP
    - Source Port
    - Destination Port
  - UDP
    - Source Port
    - Destination Port
- The evaluator shall verify that each rule can identify the following actions: permit or drop with the option to log the operation.
- The evaluator shall verify that the TSS identifies all interface types subject to the stateful packet filtering policy and explains how rules are associated with distinct network interfaces.

#### Evaluator Findings:

- The evaluator reviewed the TSS '**Section FFW\_RUL\_EXT.1**' to ensure that it describes a stateful packet filtering policy, and the following attributes are identified as being configurable within stateful traffic filtering rules for the associated protocols:
  - ICMPv4
    - Type
    - Code
  - ICMPv6
    - Type
    - Code
  - IPv4
    - Source address
    - Destination Address
    - Transport Layer Protocol
  - IPv6
    - Source address
    - Destination Address

- Transport Layer Protocol and where defined by the ST author, Extension Header Type, Extension Header Fields
  - TCP
    - Source Port
    - Destination Port
  - UDP
    - Source Port
    - Destination Port
  - The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that each rule can identify the following actions: permit or drop with the option to log the operation.
  - The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it identifies all interface types subject to the stateful packet filtering policy and explains how rules are associated with distinct network interfaces. The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**  
Upon investigation, the evaluator found that the TSS states that:
    - **The TOE administrator can define rules to permit or drop traffic based on the following parameters:**
      - **ICMPv4 Type, Code**
      - **ICMPv6: Type, Code**
      - **IPv4: Source address, Destination Address, Transport Layer Protocol**
      - **IPv6: Source address, Destination Address, Transport Layer Protocol**
      - **TCP: Source Port, Destination Port, UDP, Source Port, Destination Port**
      - **TOE network interface.**
- The administrator can define whether packets processed by the rules are logged.**
- **All network interfaces on the TOE use RJ45 ethernet cables and have the ability to perform packet filtering on packets being received or sent to the external network. Due to this, there is only one distinct network interface type where firewall rules can be configured.**

**Verdict:**

**PASS.**

5.1.9.4 FFW\_RUL\_EXT.1.2/FFW\_RUL\_EXT.1.3/FFW\_RUL\_EXT.1.4 AGD

**Objective:**

The evaluators shall verify that the guidance documentation identifies the following attributes as being configurable within stateful traffic filtering rules for the associated protocols:

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - Source address
  - Destination Address

- Transport Layer Protocol
- IPv6

Source address

- Destination Address
- Transport Layer Protocol and where defined by the ST author, Extension Header Type, Extension Header Fields
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

- The evaluator shall verify that the guidance documentation indicates that each rule can identify the following actions: permit, drop, and log.
- The evaluator shall verify that the guidance documentation explains how rules are associated with distinct network interfaces.

**Evaluator Findings:**

- The evaluator checked the AGD **Section ‘Extended Access List command format’** and ensured that it identifies the following attributes as being configurable within stateful traffic filtering rules for the associated protocols:

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - Source address
  - Destination Address
  - Transport Layer Protocol

● IPv6

Source address

- Destination Address
- Transport Layer Protocol and where defined by the ST author, Extension Header Type, Extension Header Fields
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

- The evaluator checked the AGD **Section ‘Extended Access List command format’** and ensured that it indicates that each rule can identify the following actions: permit, drop, and log.
- The evaluator checked the AGD **Section ‘Extended Access List command format’** and ensured that it explains how rules are associated with distinct network interfaces.

**AGD Section 12.2.1. Extended Access List command format**

Upon investigation, the evaluator found that the AGD activity states that:

**The following discusses settings for Extended ACLs**

**Layer 4 filtering**

**TRAIN-011(config)# access-list**

**TRAIN-011(config)# access-list [100-200] [permit | deny]**

**<0-255> An IP protocol number (0..255)**

**esp Encapsulation Security Payload**

**icmp Internet Control Message Protocol**

**igmp Internet Gateway Message Protocol**

**ip Any Internet Protocol**

**ipv6 Any Internet Protocol Version 6**

**ospf OSPF routing protocol**

**tcp Transmission Control Protocol**

**udp User Datagram Protocol**

After selecting 'permit' or 'deny', a mix of layer 3 and layer 4 protocols are available for selection. Here, the listed layer 4 protocols (esp, icmp, igmp, ospf, tcp, udp, <protocol numbers>) relate to ipv4 packets only.

**IPv4 example:**

**access-list 100 permit ipv4 udp 192.168.100.0/24 eq 8080 any log**

This access list permits accesses to UDP port 8080 from hosts in the CIDR domain 192.168.100.0/24, and to any ipv4 destination host. If the rule is matched, the result is logged.

**Selecting Layer 4 filters for IPv4:**

**TRAIN-011(config)# access-list 100 permit ipv4**

**<0-255> An IP protocol number (0..255)**

**esp Encapsulation Security Payload**

**icmpv6 Internet Control Message Protocol Version 6e ip Any Internet Protocol**

**ospf OSPF routing protocol**

**tcp Transmission Control Protocol**

**udp User Datagram Protocol**

**IPv6 example:**

**access-list 100 permit ipv6 udp 2001::1/64 eq 8080 any log**

This access list permits accesses to UDP port 8080 from hosts in the CIDR domain 2001::1/64, and to any ipv6 destination host. If the rule is matched, the result is logged.

- The evaluator shall verify that the guidance documentation explains how rules are associated with distinct network interfaces.

The relevant information is found in the following section(s): **13.3 Access list logging**

Upon investigation, the evaluator found that the AGD states : **Access-lists are assigned to a distinct network interface by the administrator.**

## Verdict:

PASS.

### 5.1.9.5 FFW\_RUL\_EXT.1.5 TSS

#### Objective:

- The evaluator shall verify that the TSS identifies the protocols that support stateful session handling. The TSS shall identify TCP, UDP, and, if selected by the ST author, also ICMP.
- The evaluator shall verify that the TSS describes how stateful sessions are established (including handshake processing) and maintained.
- The evaluator shall verify that for TCP, the TSS identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags.
- The evaluator shall verify that for UDP, the TSS identifies and describes the following attributes in session determination: source and destination addresses, source and destination ports.
- The evaluator shall verify that for ICMP (if selected), the TSS identifies and describes the following attributes in session determination: source and destination addresses, other attributes chosen in FFW\_RUL\_EXT.1.5.
- The evaluator shall verify that the TSS describes how established stateful sessions are removed.
- The TSS shall describe how connections are removed for each protocol based on normal completion and/or timeout conditions.
- The TSS shall also indicate when session removal becomes effective (e.g., before the next packet that might match the session is processed).

#### Evaluator Findings:

- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it identifies the protocols that support stateful session handling.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it identifies TCP, UDP, and, if selected by the ST author, also ICMP.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it describes how stateful sessions are established (including handshake processing) and maintained.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that, for the TCP, it identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that, for the UDP, it identifies and describes the following attributes in session determination: source and destination addresses, source and destination ports.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that, for ICMP (if selected), it identifies and describes the following attributes in session determination: source and destination addresses, other attributes chosen in FFW\_RUL\_EXT.1.5.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it describes how established stateful sessions are removed.
- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it describes how connections are removed for each protocol based on normal completion and/or timeout conditions.

- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it indicates when session removal becomes effective (e.g., before the next packet that might match the session is processed)

The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that:

- **TCP, UDP, and ICMP packets for established sessions will be allowed without applying the stateful traffic filtering rules based on the parameters defined in FFW\_RUL\_EXT.1.5.**
- **The TOE features a packet filtering capability using stateful Access Control List (ACL) rules configured with the access-list configuration command and interface ip access-group [in|out] settings for IPv4 and IPv6 network traffic. When ACL rules are applied to an interface with the ip access-group [in|out] configuration command, the ACL is either applied to inbound or outbound traffic, depending on the [in|out] option. If an inbound ACL is applied to an interface, inbound packet traffic is checked against the ACL rules applied to that interface, and either allowed or dropped depending on the configuration of the matching rule before any further processing of the packet occurs (such as routing, etc.). If an outbound ACL is applied to an interface, then any packets that are queued to be sent out an interface are checked against the configured ACL and either allowed to be sent or dropped at the outbound interface.**
- **Packets that are allowed through any inbound ACL are then checked against the stateful session table to see if there is an existing session to which the packet belongs. Packet information such as source and destination IP address, source and destination ports, protocol, and flags unique to protocols are used to determine if the packet belongs to an existing session or not. If no existing session matches the packet, a new session is created.**
- **The TOE will keep track of stateful sessions in the table until either the protocol ends the session (such as TCP-FIN or TCP-RST packets) or after an amount of time has lapsed (timeout period) where no packet was matched against the session. The exact timeout period depends on the session type and current state of the session and is not configurable. Examples: ICMP and ICMPv6 is 30 seconds, TCP sessions in the FIN WAIT state is 120 seconds, etc**

**Verdict:**

**PASS.**

**5.1.9.6 FFW\_RUL\_EXT.1.5 AGD**

**Objective:**

- The evaluator shall verify that the guidance documentation describes stateful session behaviours. For example, a TOE might not log packets that are permitted as part of an existing session.

**Evaluator Findings:**

- The evaluator checked the AGD and ensured that it describes stateful session behaviours.

The relevant information is found in the following section(s): **AGD Section 13 'ACL Guide for KlasOS Firewall' and Section 14 Connection tracking in KlasOS Firewall using ACLs.**

Upon investigation, the evaluator found that the AGD states that: **The updates extend the existing 'extended' ACL configuration set.**

**Extended ACL format:**

**access-list <100-199> <action> <protocol> <ip options, tcp/udp ports> <protocol options>**

**access-list <100-199> <action> ipv6 <protocol> <ip options, tcp/udp ports> <protocol options>**

**This update will add 'conn' to the list of protocol options to enable connection tracking rules:**

**TRAIN-011(config)# access-list 100 permit tcp any any conn**

(INVALID|ESTABLISHED|NEW|RELATED|UNTRACKED|SNAT|DNAT) Any combination of the list in double quotes and separated with a comma

TRAIN-011(config)# access-list 100 permit ipv6 tcp any any conn

(INVALID|ESTABLISHED|NEW|RELATED|UNTRACKED|SNAT|DNAT) Any combination of the list in double quotes and separated with a comma

The TOE provides configuration for logging the packets that are permitted as part of the existing session.

**Verdict:**

PASS.

5.1.9.7 FFW\_RUL\_EXT.1.6 TSS

**Objective:**

- The evaluator shall verify that the TSS identifies the following as packets that will be automatically dropped and are counted or logged:
  - a) Packets which are invalid fragments, including a description of what constitutes an invalid fragment.
  - b) Fragments that cannot be completely re-assembled
  - c) Packets where the source address is defined as being on a broadcast network.
  - d) Packets where the source address is defined as being on a multicast network.
  - e) Packets where the source address is defined as being a loopback address.
  - f) The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4;
  - g) The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6;
  - h) Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.
  - i) Other packets defined in FFW\_RUL\_EXT.1.6 (if any)

**Evaluator Findings:**

- The evaluator reviewed the TSS **Section ‘FFW\_RUL\_EXT.1** to ensure that it identifies the following as packets that will be automatically dropped and are counted or logged:
  - a) Packets which are invalid fragments, including a description of what constitutes an invalid fragment.
  - b) Fragments that cannot be completely re-assembled
  - c) Packets where the source address is defined as being on a broadcast network.
  - d) Packets where the source address is defined as being on a multicast network.
  - e) Packets where the source address is defined as being a loopback address.
  - f) The TSF rejects and is capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4;
  - g) The TSF rejects and is capable of logging network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6;

- h) Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.
- i) Other packets defined in FFW\_RUL\_EXT.1.6 (if any).

The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE also has default stateful traffic filtering rules for dropping packets. These rules are defined in FFW\_RUL\_EXT.1.6. Logging or counting will be performed on these packets.**

**Verdict:**

**PASS.**

5.1.9.8 FFW\_RUL\_EXT.1.6 AGD

**Objective:**

- The evaluator shall verify that the guidance documentation describes packets that are discarded and potentially logged by default. If applicable protocols are identified, their descriptions need to be consistent with the TSS.
- If logging is configurable, the evaluator shall verify that applicable instructions are provided to configure auditing of automatically rejected packets.

**Evaluator Findings:**

- The evaluator checked the AGD **Section 15 'Firewall 'ip|ipv6 security' and section 15.1 'Setting Overview'** settings and ensured that it describes packets that are discarded and potentially logged by default. If applicable protocols are identified, their descriptions need to be consistent with the TSS.
- The evaluator checked the AGD Section **'Firewall 'ip|ipv6 security',' Setting Overview'** and ensured that, if logging is configurable, that applicable instructions are provided to configure auditing of automatically rejected packets.

The relevant information is found in the following section(s) **AGD Section 15. Firewall 'ip|ipv6 security' settings** and **Section 15.1 Setting Overview**.

Upon investigation, the evaluator found that the AGD states that: **Some firewall requirements can be said to be standalone in that there is a specific way to meet the requirement and rules based on the requirement don't need to be possibly combined with other flow attributes since they talk about invalid IP addressing. 'ip|ipv6' security settings allow:**

- selecting these rules for early matching,
- reverse path routing check for interfaces
- early packet fragment matching for ipv4 and ipv6
- rate-limiting ACL selected flows

**TRAIN-011(config-if)# ip security drop [in|out] special-purpose [saddr|daddr]**

- ip|ipv6 security verify reverse-path log <prefix>
- ip|ipv6 security drop [in|out] special-purpose [saddr|daddr] [mask] log <prefix>
- ipv6 security drop in exthdrs [mask] log <prefix> log <prefix>

Further the AGD also states the following setting for invalid fragments, fragments that cannot be re-assembled completely and packets with IP options:

Setting	Firewall Requirements	Comment
---------	-----------------------	---------



ip security drop in fragments <prefix>	<ul style="list-style-type: none"> <li>• Firewall rule to drop packets that are invalid fragments</li> <li>• Firewall rule to drop fragments that cannot be completely re-assembled</li> </ul>	This has been added to filter out any fragmented packets that may or may not be part of a session
access-list 100 deny ip any any advanced raw ipv4options [option] <prefix>	<ul style="list-style-type: none"> <li>• Firewall rule to filter ipv4 traffic with loose source, strict source and record routing</li> </ul>	[option] – specifies which type of routing to filter 3 = loose source 7 = record route 9 = strict source routing

**Verdict:**

PASS.

5.1.9.9 FFW\_RUL\_EXT.1.7 TSS

**Objective:**

- The evaluator shall verify that the TSS explains how the following traffic can be dropped and counted or logged:
  - a) Packets where the source address is equal to the address of the network interface where the network packet was received.
  - b) Packets where the source or destination address of the network packet is a link-local address.
  - c) Packets where the source address does not belong to the networks associated with the network interface where the network packet was received, including a description of how the TOE determines whether a source address belongs to a network associated with a given network interface.

**Evaluator Findings:**

- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it explains how the following traffic can be dropped and counted or logged:
- Packets where the source address is equal to the address of the network interface where the network packet was received.
- Packets where the source or destination address of the network packet is a link-local address.
- Packets where the source address does not belong to the networks associated with the network interface where the network packet was received, including a description of how the TOE determines whether a source address belongs to a network associated with a given network interface.

The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that:

**There is an integrated firewall ruleset that can be applied when the packets have a source address equal to the address of the network interface where the packet was received. It must be configured for IPv4 and IPv6 separately. This configuration allows the security administrator to specify valid IP address ranges for the source address of incoming packets. At the end of the firewall ruleset, there is a default-deny that will reject any packets with an invalid source address.**

**There is also an integrated firewall ruleset that can be applied when the source or destination address of the network packet is a link-local address.**

**Verdict:**

**PASS.**

5.1.9.10 FFW\_RUL\_EXT.1.7 AGD

**Objective:**

- The evaluator shall verify that the guidance documentation describes how the TOE can be configured to implement the required rules.
- If logging is configurable, the evaluator shall verify that applicable instructions are provided to configure auditing of automatically rejected packets.

**Evaluator Findings:**

- The evaluator checked the AGD **Section ‘Firewall ‘ip|ipv6 security’ settings ‘,’Setting Overview ‘**and ensured that it describes how the TOE can be configured to implement the required rules.
- The evaluator checked the AGD **Section ‘Firewall ‘ip|ipv6 security’ settings ‘,’Setting Overview’** and ensured that, if logging is configurable, it provides applicable instructions to configure auditing of automatically rejected packets.

**AGD Section 14. Firewall ‘ip|ipv6 security’ settings and Section 14.1 Setting Overview**

Upon investigation, the evaluator found that the AGD activity states that:

Setting	Firewall Requirements	Comment
ip ipv6 security verify reverse-path log <prefix>	<ul style="list-style-type: none"> <li>• packets with source address on the broadcast (ipv4) network for the interface should be dropped.</li> <li>• packets with source address equal to the interface should be dropped.</li> <li>• Packets with source address which cannot be routed back through the interface should be dropped</li> </ul>	<p>broadcast address doesn’t exist for ipv6 (multicast is used).</p> <p>For the routing requirement, the KlasOS routing table is looked up to verify whether the packet is routable back out the interface. If a default route is present for the interface, then the packet will not be dropped.</p>
ip ipv6 security drop [in out] special-purpose [saddr daddr] [mask] log <prefix>	<ul style="list-style-type: none"> <li>• packets with multicast source address</li> <li>• link local match</li> <li>• loopback match</li> <li>• ‘unspecified’, reserved for future use (ipv4)</li> <li>• ‘unspecified’, reserved for future use (ipv6)</li> </ul>	<p>[in out] - block ingress or egress traffic</p> <p>[saddr daddr] - packet source or destination address is matched</p> <p>[mask] - select iana/multicast networks to block (more info below)</p>
show [ip ipv6] security interface <iface type/name>	<ul style="list-style-type: none"> <li>• Ability to see rule counters being hit per interface</li> </ul>	<p>This output can be quite large even for a small number of settings.</p>

**Verdict:**

PASS.

#### 5.1.9.11 FFW\_RUL\_EXT.1.8 TSS [TD0545]

##### Objective:

- The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.

"If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the TSS shall describe the underlying mechanism."

##### Evaluator Findings:

- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset. If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the TSS shall describe the underlying mechanism

The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that:

**The TOE stores ACL rules in the order they were configured. This is the same order the rules are checked when checking an inbound or outbound packet. Whenever any ACL is applied to an interface, a default DROP policy rule is applied for that interface as the last rule. This will drop any packet that didn't match any other rule in the applied ACL. For example, if an ACL is applied in the outbound direction, then by default, an outbound packet that didn't match any rules will be dropped by default. If there are conflicting rules configured, the first rule in the list will be processed.**

**Packets that are allowed through any inbound ACL are then checked against the stateful session table to see if there is an existing session to which the packet belongs. Packet information such as source and destination IP address, source and destination ports, protocol, and flags unique to protocols are used to determine if the packet belongs to an existing session or not. If no existing session matches the packet, a new session is created.**

##### Verdict:

PASS.

#### 5.1.9.12 FFW\_RUL\_EXT.1.8 AGD

##### Objective:

- The evaluator shall verify that the guidance documentation describes how the order of stateful traffic filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.

##### Evaluator Findings:

- The evaluator checked the AGD **Section 'Extended Access lists'** and ensured that it describes how the order of stateful traffic filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.

The relevant information is found in the following section(s) **AGD Section 12.2. Extended Access lists**

Upon investigation, the evaluator found that the AGD states that:

- **These access lists may be used to filter IPv4 and IPv6 traffic. They are also capable of filtering TCP, UDP, ICMP and other IP protocols. They are selected by using access-list number 100-199.**

- The access-list logging feature provides the ability to log messages about packets that are permitted or denied by either a standard or an extended IP access list.
- Any packet that matches the access list rules causes an information log message about the packet to be sent to the system log.
- Log messages include information about the access list number, the source and destination IP address and ports of packets and the incoming and/or outgoing interface.
- Further AGD Section 15 'Firewall 'ip|ipv6 security' settings' states that:

**Note:** The TOE stores ACL rules in the order they were configured. This is the same order the rules are checked when checking an inbound or outbound packet.

**Verdict:**

**PASS.**

#### 5.1.9.13 FFW\_RUL\_EXT.1.9 TSS

**Objective:**

- The evaluator shall verify that the TSS describes the process for applying stateful traffic filtering rules and also that the behavior (either by default, or as configured by the administrator) is to deny packets when there is no rule match unless another required condition allows the network traffic (i.e., FFW\_RUL\_EXT.1.5 or FFW\_RUL\_EXT.2.1).

**Evaluator Findings:**

- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it describes the process for applying stateful traffic filtering rules and also that the behavior (either by default, or as configured by the administrator) is to deny packets when there is no rule match unless another required conditions allows the network traffic (i.e., FFW\_RUL\_EXT.1.5 or FFW\_RUL\_EXT.2.1).

The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that:

**The TOE features a packet filtering capability using stateful Access Control List (ACL) rules configured with the access-list configuration command and interface ip access-group [in|out] settings for IPv4 and IPv6 network traffic. When ACL rules are applied to an interface with the ip access-group [in|out] configuration command, the ACL is either applied to inbound or outbound traffic, depending on the [in|out] option. If an inbound ACL is applied to an interface, inbound packet traffic is checked against the ACL rules applied to that interface, and either allowed or dropped depending on the configuration of the matching rule before any further processing of the packet occurs (such as routing, etc.). If an outbound ACL is applied to an interface, then any packets that are queued to be sent out an interface are checked against the configured ACL and either allowed to be sent or dropped at the outbound interface.**

**The TOE stores ACL rules in the order they were configured. This is the same order the rules are checked when checking an inbound or outbound packet. Whenever any ACL is applied to an interface, a default DROP policy rule is applied for that interface as the last rule. This will drop any packet that didn't match any other rule in the applied ACL. For example, if an ACL is applied in the outbound direction, then by default, an outbound packet that didn't match any rules will be dropped by default. If there are conflicting rules configured, the first rule in the list will be processed.**

**Verdict:**

**PASS.**

#### 5.1.9.14 FFW\_RUL\_EXT.1.9 AGD

##### Objective:

- The evaluator shall verify that the guidance documentation describes the behavior if no rules or special conditions apply to the network traffic.
- If the behavior is configurable, the evaluator shall verify that the guidance documentation provides the appropriate instructions to configure the behavior to deny packets with no matching rules.

##### Evaluator Findings:

- The evaluator checked the AGD **Section 13.2.1 'Extended Access List command format'** and ensured that it describes the behavior if no rules or special conditions apply to the network traffic.
- The evaluator checked the AGD **Section 13.2.1 'Extended Access List command format'** and ensured that it provides the appropriate instructions to configure the behavior to deny packets with no matching rules.

##### **12.2.1. Extended Access List command format**

Upon investigation, the evaluator found that the AGD states that: **The following discusses settings for Extended ACLs**

##### **Layer 4 filtering**

```
TRAIN-011(config)# access-list
```

```
TRAIN-011(config)# access-list [100-200] [permit|deny]
```

```
<0-255> An IP protocol number (0..255)
```

```
esp Encapsulation Security Payload
```

```
icmp Internet Control Message Protocol
```

```
igmp Internet Gateway Message Protocol
```

```
ip Any Internet Protocol
```

```
ipv6 Any Internet Protocol Version 6
```

```
ospf OSPF routing protocol
```

```
tcp Transmission Control Protocol
```

```
udp User Datagram Protocol
```

After selecting 'permit' or 'deny', a mix of layer 3 and layer 4 protocols are available for selection. Here, the listed layer 4 protocols (esp, icmp, igmp, ospf, tcp, udp, <protocol numbers>) relate to ipv4 packets only.

IPv4 example:

```
access-list 100 permit ipv6 udp 192.168.100.0/24 eq 8080 any log
```

This access list permits accesses to UDP port 8080 from hosts in the CIDR domain 192.168.100.0/24, and to any ipv4 destination host. If the rule is matched, the result is logged.

Selecting Layer 4 filters for IPv6:

```
TRAIN-011(config)# access-list 100 permit ipv6
```

```
<0-255> An IP protocol number (0..255)
```

```
esp Encapsulation Security Payload
```

```
icmpv6 Internet Control Message Protocol Version 6
```

**ip** Any Internet Protocol  
**ospf** OSPF routing protocol  
**tcp** Transmission Control Protocol  
**udp** User Datagram Protocol

**IPv6 example:**

```
access-list 100 permit ipv6 udp 2001::1/64 eq 8080 any log
```

This access list permits accesses to UDP port 8080 from hosts in the CIDR domain 2001::1/64, and to any ipv6 destination host. If the rule is matched, the result is logged.

- Further AGD Section 15 'Firewall 'ip|ipv6 security' settings' states that:

**Note:** If a packet is sent through the TOE that does not match the ruleset configured, that packet will be dropped.

**Verdict:**

**PASS.**

5.1.9.15 FFW\_RUL\_EXT.1.10 TSS

**Objective:**

- The evaluator shall verify that the TSS describes how the TOE tracks and maintains information relating to the number of half-open TCP connections.
- The TSS should identify how the TOE behaves when the administratively defined limit is reached and should describe under what circumstances stale half-open connections are removed (e.g. after a timer expires).

**Evaluator Findings:**

- The evaluator reviewed the TSS **Section 'FFW\_RUL\_EXT.1'** to ensure that it describes how the TOE tracks and maintains information relating to the number of half-open TCP connections.
- The TSS **Section 'FFW\_RUL\_EXT.1'** identifies how the TOE behaves when the administratively defined limit is reached and should describe under what circumstances stale half-open connections are removed (e.g. after a timer expires).

The relevant information is found in the following Section(s): TOE Summary Specification **FFW\_RUL\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **Half-open TCP connection attacks are mitigated with a synproxy option feature which can be configured with an ACL rule. This option causes the TOE to intercept new TCP connections and determines if the packet is a false SYN-ACK or ACK packet that should be dropped. Specific ports can be configured with the ACL rule as usual. This feature is either on or off and does not permit the configuration of a number of half-open TCP states allowed. The dropping if these packets is logged. The default threshold limit for half open connections on the TOE is 0.**

**Verdict:**

**PASS.**

5.1.9.16 FFW\_RUL\_EXT.1.10 AGD

**Objective:**

- The evaluator shall verify that the guidance documentation describes the behaviour of imposing TCP half-open connection limits and its default state if unconfigured.
- The evaluator shall verify that the guidance clearly indicates the conditions under which new connections will be dropped e.g. per-destination or per-client.

## Evaluator Findings:

- The evaluator checked the AGD Section ‘Mitigating TCP flood attacks using SYNPROXY feature ‘,’ How to count dropped SYN packets and SYN packets that have not been dropped’ and ensured that it describes the behavior of imposing TCP half-open connection limits and its default state if unconfigured.
- The evaluator checked the AGD and ensured that it clearly indicates the conditions under which new connections will be dropped e.g. per-destination or per-client.

The relevant information is found in the following **Section 16 Mitigating TCP flood attacks using SYNPROXY feature and 16.1. How to count dropped SYN packets and SYN packets that have not been dropped.**

Upon investigation, the evaluator found that the AGD states that:

**Synproxy intercepts new TCP connections and handles the initial 3-way handshake using syncookies instead of contrack to establish the connection. Running synproxy on a listening server port thus prevents a SYN flood attack on that port from consuming limited contrack resources. With contrack, false SYN-ACK and ACK packets can be filtered out before they hit the "listen" state lock.**

**The diagram below shows the network of a possible attack. The target is listening on port 22 (ssh). The attacker is attempting to flood the target with SYN packets The firewall has synproxy rules configured that protect port 22 which enables the ‘good user’ to establish an ssh session with the target.**

**The following example configuration can be used to protect the ssh port (port 22)**

```
access-list 100 permit tcp any any eq 22 advanced raw ct notrack
```

```
access-list 100 permit tcp any any eq 22 conn INVALID, UNTRACKED advanced forward-only synproxy wscale 7 mss 1460
```

```
ip tcp contrack strict
```

```
interface vSwitch 3
```

```
ip access-group 100 in
```

- **show ip firewall system can be used to view details of the rules and packet counters.**

## Verdict:

**PASS.**

### 5.1.10 Security management (FMT)

#### 5.1.10.1 FMT\_SMF.1/FFW Specification of Management Functions

##### Objective:

- The evaluation activities specified for FMT\_SMF.1 in the Supporting Document for the Base-PP shall be applied in the same way to the newly added management functions defined in FMT\_SMF.1/FFW in the FW Module.

##### Evaluator Findings:

- The evaluator reviewed the documentation and verified that the evaluation activities specified for FMT\_SMF.1 in the Supporting Document for the Base-PP have been applied in the same way to the newly added management functions defined in FMT\_SMF.1/FFW in the FW Module.
- The relevant information is found in the following section(s): **FMT\_SMF.1/FFW.**
- Upon investigation, the evaluator found that the documentation states that: **The administrator can configure firewall rules via the SSH command line interface both locally and remotely.**
- **Further the AGS Section 15 ‘Firewall ‘ip|ipv6 security’ settings’ states that:**

**All firewall rules can be applied to the TOE using the local or remote CLI interface. When logging in via a local interface, there will be a prompt to “Press RETURN to get started.”**

**Verdict:**

PASS.

## 5.2 Optional Requirements

### 5.2.1 Security Audit (FAU)

#### 5.2.1.1 FAU\_STG.1 Protected Audit Trail Storage

##### 5.2.1.1.1 FAU\_STG.1 TSS

**Objective:**

- The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally and how these records are protected against unauthorized modification or deletion.
- The evaluator shall ensure that the TSS describes the conditions that must be met for authorized deletion For distributed TOEs the evaluator shall examine the TSS to ensure it describes to which TOE components this SFR applies and how local storage is implemented among the different TOE components (e.g. every TOE component does its own local storage or the data is sent to another TOE component for central local storage of all audit events).

**Evaluator Findings:**

- The evaluator examined the TSS to ensure it describes the amount of audit data that are stored locally and how these records are protected against unauthorized modification or deletion.

The relevant information is found in the following section(s): TOE Summary Specification **FAU\_STG.1**.

Upon investigation, the evaluator found that the TSS states that: **Audit data is stored locally on the TOE. The audit records can't be deleted by the TOE user or Security Administrator. The action that the TOE takes when local storage is full is described in the evaluator findings for the FAU\_STG\_EXT.1 SFR.**

- **The TOE is not distributed.**

**Verdict:**

PASS.

##### 5.2.1.1.2 FAU\_STG.1 AGD

**Objective:**

- The evaluator shall examine the AGD to determine that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion.

**Evaluator Findings:**

- The evaluator examined the AGD and determined that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion.

The relevant information is found in the following section(s): **8 Logging and Auditing**

Upon investigation, the evaluator found that the AGD states that: **The locally stored audit log files cannot be modified or deleted by an unauthorized user**

**Verdict:**

PASS.



### 5.2.1.2 FAU\_STG\_EXT.3/LocSpace Action in Case of Possible Audit Data Loss

#### 5.2.1.2.1 FAU\_STG\_EXT.3/LocSpace TSS

##### Objective:

- The evaluator shall examine the TSS to ensure that it details how the Security Administrator is warned before the local storage for audit data is full.

##### Evaluator Findings:

- The evaluator examined the TSS ensured that it details how the Security Administrator is warned before the local storage for audit data is full.

The relevant information is found in the following Section(s): TOE Summary Specification

#### **FAU\_STG\_EXT.3/LocSpace**

Upon investigation, the evaluator found that the TSS states that: **The TSF generates a log entry when 75% of local flash storage capacity has been used.**

##### Verdict:

**PASS.**

#### 5.2.1.2.2 FAU\_STG\_EXT.3/LocSpace AGD

##### Objective:

- The evaluator shall also ensure that the AGD describes how the Security Administrator is warned before the local storage for audit data is full and how this warning is displayed or stored (since there is no guarantee that an administrator session is running at the time the warning is issued, it is probably stored in the log files). The description in the AGD shall correspond to the description in the TSS.

##### Evaluator Findings:

- The evaluator ensured that the **AGD Section 'Logging and Auditing'** describes how the Security Administrator is warned before the local storage for audit data is full and how this warning is displayed or stored (since there is no guarantee that an administrator session is running at the time the warning is issued, it is probably stored in the log files). The description in the AGD corresponds to the description in the TSS.

The relevant information is found in the following section(s) **AGD Section 8 Logging and Auditing**

Upon investigation, the evaluator found that the AGD states that: **There is a log entry when the file system flash storage is 75% full.**

##### Verdict:

**PASS.**

### 5.2.2 Cryptographic Support (FCS)

#### 5.2.2.1 FCS\_DTLSC\_EXT.2 Extended: DTLS Client Support for Mutual Authentication

##### 5.2.2.1.1 FCS\_DTLSC\_EXT.2.1 TSS

##### Objective:

- The evaluator shall ensure that the TSS description required per FIA\_X509\_EXT.2.1 includes the use of client-side certificates for DTLS mutual authentication.

##### Evaluator Findings:

- The evaluator ensured that the TSS description required per FIA\_X509\_EXT.2.1 includes the use of client-side certificates for DTLS mutual authentication.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports DTLS mutual authentication and will send its DTLS client-side certificate upon request from a DTLS Server. To initiate a DTLS connection the TOE will send a client hello message. When the hello verify request message is received, the TOE performs a stateless cookie exchange to ensure the DTLS server is not being spoofed. When certificates are exchanged the TOE will confirm that the hostnames match. If the hostnames don't match the DTLS session will not be established.**

**Verdict:**

**PASS.**

5.2.2.1.2 *FCS\_DTLSC\_EXT.2.1 AGD*

**Objective:**

- If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD includes instructions for configuring the client-side certificates for DTLS mutual authentication.

**Evaluator Findings:**

- The TSS Section that mutual authentication using X.509v3 certificates is used, the evaluator verified that the AGD includes instructions for configuring the client-side certificates for DTLS mutual authentication.

The relevant information is found in the **AGD Section 10. Introduction to Certificate Manager.**

Upon investigation, the evaluator found that the AGD states that: **Section 10.1 Generating and Adding Certificates to a Certificate Manager' of the AGD includes instructions for configuring client-side certificates for DTLS mutual authentication.**

**Verdict:**

**PASS.**

5.2.2.1.3 *FCS\_DTLSC\_EXT.2.2 TSS*

**Objective:**

- The evaluator shall verify that the TSS describes the actions that take place if a message received from the DTLS Server fails the MAC integrity check.

**Evaluator Findings:**

- The evaluator verified that the TSS **Section 'FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2'** describes the actions that take place if a message received from the DTLS Server fails the MAC integrity check.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **During internal channel communication between the client and server, if there is a message authentication code (MAC) verification failure, the TOE will silently discard the record and continue with the connection. Key establishment is performed using RSA with 2048 bits, 3072 bits, or 4096 bits.**

**Verdict:**

**PASS.**

#### 5.2.2.1.4 FCS\_DTLSC\_EXT.2.3 TSS

##### Objective:

- The evaluator shall verify that the TSS describes how replay is detected and silently discarded for DTLS records that have previously been received and too old to fit in the sliding window.

##### Evaluator Findings:

- The evaluator verified that the TSS **Section 'FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2'** describes how replay is detected and silently discarded for DTLS records that have previously been received and too old to fit in the sliding window.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **Valid record sequence numbers are maintained in a sliding window. For each record received, the TOE verifies if it is in the window boundary. Messages that are received where the same record was previously received or that are too old to fit in the sliding window are silently discarded.**

##### Verdict:

PASS.

#### 5.2.2.2 FCS\_DTLSS\_EXT.2 Extended: DTLS Server Support for Mutual Authentication

##### 5.2.2.2.1 FCS\_DTLSS\_EXT.2.1 and FCS\_DTLSS\_EXT.2.2 TSS

##### Objective:

- The evaluator shall ensure that the TSS description required per FIA\_X509\_EXT.2.1 includes the use of client-side certificates for DTLS mutual authentication.
- The evaluator shall verify the TSS describes how the TSF uses certificates to authenticate the DTLS client.
- The evaluator shall verify the TSS describes whether the TSF supports any fallback authentication functions (e.g. username/password, challenge response) the TSF uses to authenticate DTLS clients that do not present a certificate. If fallback authentication functions are supported, the evaluator shall verify the TSS describes whether the fallback authentication functions can be disabled.

##### Evaluator Findings:

- The evaluator ensured that the TSS description required per FIA\_X509\_EXT.2.1 includes the use of client-side certificates for DTLS mutual authentication.

The relevant information is found in the following section(s): TOE Summary Specification '**FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2'**

Upon investigation, the evaluator found that the TSS states that: **The TOE requires supports DTLS mutual authentication and will request the client-side certificate.**

- The evaluator verified the TSS describes how the TSF uses certificates to authenticate the DTLS client.

The relevant information is found in the following section(s): TOE Summary Specification '**FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2'**

Upon investigation, the evaluator found that the TSS states that: **Upon receiving the client hello message, the TOE sends a hello verify request message and performs a stateless cookie exchange to ensure the DTLS client IP address is not being spoofed. When certificates are exchanged, the TOE will confirm that the FQDN, IPv4 or IPv6 identifier in the CN/SAN matches in the certificate. If the FQDN, IPv4 or IPv6 identifier in the CN/SAN**

**doesn't match, the DTLS session will not be established. If a SAN and CN are both present in a certificate, SAN takes priority no matter the circumstance.**

- The evaluator verified the TSS describes whether the TSF supports any fallback authentication functions (e.g. username/password, challenge response) the TSF uses to authenticate DTLS clients that do not present a certificate. If fallback authentication functions are supported, the evaluator verified the TSS describes whether the fallback authentication functions can be disabled.

The relevant information is found in the following section(s): TOE Summary Specification '**FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**'

- Upon investigation, the evaluator found that the TSS states that: **Fallback authentication is not supported for DTLS.**

**Verdict:**

**PASS.**

**5.2.2.2.2 FCS\_DTLSS\_EXT.2.3 TSS**

**Objective:**

- The evaluator shall verify that the TSS describes which types of identifiers are supported for during client authentication (e.g. Fully Qualified Domain Name (FQDN)). If FQDNs are supported, the evaluator shall verify that the TSS describes that corresponding identifiers are matched according to RFC6125. For all other types of identifiers, the evaluator shall verify that the TSS describes how these identifiers are parsed from the certificate, what the expected identifiers are and how the parsed identifiers from the certificate are matched against the expected identifiers.

**Evaluator Findings:**

- The evaluator verified that the TSS Section' describes which types of identifiers are supported during client authentication (e.g. Fully Qualified Domain Name (FQDN)). If FQDNs are supported, the evaluator verified that the TSS describes that corresponding identifiers are matched according to RFC6125. For all other types of identifiers, the evaluator verified that the TSS describes how these identifiers are parsed from the certificate, what the expected identifiers are and how the parsed identifiers from the certificate are matched against the expected identifiers.

The relevant information is found in the following Section(s): TOE Summary Specification '**FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**'

Upon investigation, the evaluator found that the TSS states that: **During Client Authentication only FQDN and IPv4/IPv6 Addresses are supported as identifiers. FQDN input is via an XML defined input field and supports CN-ID, DNS-ID and SRV-ID (per RFC6125), input restrictions prevent application of spaces in text input, characters are limited to (A-Z/a-z/\_/./). URI-ID format is not supported. IPv4/6 addresses are parsed from an XML input field with restricted input (IPv4:"0-9/.", IPv6:"0-9/A-F/a-f/:")) and matched against expected identifiers (verification that input is compliant with IPv4/IPv6 format) via the netaddr library for python, which receives data from XML input. Within the CN, ip conversion is performed via the inet\_ntop function of the standard C++ suite.**

**Verdict:**

**PASS.**

#### 5.2.2.2.3 FCS\_DTLSS\_EXT.2.1 and FCS\_DTLSS\_EXT.2.2 AGD

##### Objective:

- If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD includes instructions for configuring the client-side certificates for DTLS mutual authentication.
- The evaluator shall verify the AGD describes how to configure the DTLS client certificate authentication function. If the TSF supports fallback authentication functions, the evaluator shall verify the AGD provides instructions for configuring the fallback authentication functions. If fallback authentication functions can be disabled, the evaluator shall verify the AGD provides instructions for disabling the fallback authentication functions.

##### Evaluator Findings:

- The evaluator verified that the AGD Section **11.1.1.2. Configuring client-side certificates for Mutual Authentication** includes instructions for configuring the client-side certificates for DTLS mutual authentication.
- The evaluator verified the AGD Section **11.1.1.2. Configuring client-side certificates for Mutual Authentication and 11.1. encryption-mode setting** describes how to configure the DTLS client certificate authentication function. If the TSF supports fallback authentication functions, the evaluator verified the AGD provides instructions for configuring the fallback authentication functions. If fallback authentication functions can be disabled, the evaluator verified the AGD provides instructions for disabling the fallback authentication functions.

The relevant information is found in **Section 11.1.1.2. Configuring client-side certificates for Mutual Authentication and 11.1. encryption-mode setting**

Upon investigation, the evaluator found that the AGD **Section 11.1.1** states that: **Fallback authentication is not supported for DTLS.**

##### Verdict:

PASS.

#### 5.2.2.2.4 FCS\_DTLSS\_EXT.2.3 AGD

##### Objective:

- The evaluator shall ensure that the AGD describes the configuration of expected identifier(s) for X.509 certificate-based authentication of DTLS clients. The evaluator ensures this description includes all types of identifiers described in the TSS and, if claimed, configuration of the TOE to use a directory server.
- The evaluator shall send a client certificate with an identifier that does not match an expected identifier and verify that the server denies the connection.

##### Evaluator Findings:

- The evaluator ensured that the AGD Section describes the configuration of expected identifier(s) for X.509 certificate-based authentication of DTLS clients. The evaluator ensures this description includes all types of identifiers described in the TSS and, if claimed, configuration of the TOE to use a directory server.
- The relevant information is found in the following section(s): **'Configuring a reference identifier for a trustpoint'**
- The evaluator sent a client certificate with an identifier that does not match the expected identifier and verify that the server denies the connection.

The relevant information is found in the following section(s): **AGD Section 10.1 SubSection 9 'Configuring a reference identifier for a trustpoint'**

Upon investigation, the evaluator found that the AGD states that:

KlasOS(cert-tp-mytruspoint)# reference-id FQDN (FQDN or IPv4/IPv6)

KlasOS(cert-tp-mytruspoint)# validation identifier-check (strict/basic)

Note: "validation identifier-check" should always be set to "strict" in the Common Criteria configuration. The TOE supports both IPv4 and IPv6 as well as FQDN in the CN/SAN of a certificate. SAN always takes priority if it is present in the certificate.

**Verdict:**

PASS.

## 5.3 Selection-Based Requirements

### 5.3.1 Cryptographic Support (FCS)

5.3.1.1 FCS\_DTLSC\_EXT.1 Extended: DTLS Client Protocol Without Mutual Authentication

5.3.1.1.1 FCS\_DTLSC\_EXT.1.1 TSS

**Objective:**

- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified.
- The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.

**Evaluator Findings:**

- The evaluator checked the description of the implementation of this protocol in the TSS and ensured that the ciphersuites supported are specified.

The relevant information is found in the following Section(s): TOE Summary Specification : **FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2**

- The evaluator checked the TSS and ensured that the ciphersuites specified include those listed for this component.

The relevant information is found in the following Section(s): TOE Summary Specification : FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2

Upon investigation, the evaluator found that the TSS states that: **The TOE supports DTLS 1.2 to allow two TOEs to be connected in a SD-WAN and supports both client and server. The following ciphersuites are supported:**

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA;  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA;  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256;  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256;  
TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256; and  
TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384.

**Verdict:**

PASS.

#### 5.3.1.1.2 FCS\_DTLSC\_EXT.1.2 TSS

##### Objective:

- The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application- configured reference identifier, including which types of reference identifiers are supported (e.g. application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.

##### Evaluator Findings:

- The evaluator ensured that the TSS describes the client's method of establishing all reference identifiers from the administrator/application- configured reference identifier, including which types of reference identifiers are supported (e.g. application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports reference identifiers using FQDN, IPv4 and IPv6 in the CN or SAN of the certificate. Wildcards are not supported for any type of reference identifier. To initiate a DTLS connection the TOE will send a client hello message. When the hello verify request message is received, the TOE performs a stateless cookie exchange to ensure the DTLS server is not being spoofed. When certificates are exchanged the TOE will confirm that the hostnames match. If the hostnames don't match the DTLS session will not be established.**

##### Verdict:

PASS.

#### 5.3.1.1.3 FCS\_DTLSC\_EXT.1.4 TSS

##### Objective:

- The evaluator shall verify that TSS describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behaviour is performed by default or may be configured.

##### Evaluator Findings:

- The evaluator verified that TSS Section describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behaviour is performed by default or may be configured.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSC\_EXT.1 & FCS\_DTLSC\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **The TOE does not support Elliptic Curves or Group Extensions.**

##### Verdict:

PASS.

#### 5.3.1.1.4 FCS\_DTLSC\_EXT.1.1 AGD

##### Objective:

- The evaluator shall also check the AGD to ensure that it contains instructions on configuring the TOE so that DTLS conforms to the description in the TSS.

##### Evaluator Findings:

- The evaluator also checked the AGD Section and ensured that it contains instructions on configuring the TOE so that DTLS conforms to the description in the TSS.

The relevant information is found in the following section(s): **Section 11.1.1 encryption-mode pki-DTLS**

Upon investigation, the evaluator found that the AGD states that: **When the TOE is configured to be in a CC compliant configuration, DTLSv1.2 is the only accepted version of DTLS.**

**The only ciphers supported for this DTLS mode are the following:**

- **TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA** as defined in RFC 3268,
- **TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA** as defined in RFC 3268,
- **TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256** as defined in RFC 5246,
- **TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256** as defined in RFC 5246,
- **TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256** as defined in RFC 5288,
- **TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384** as defined in RFC 5288

**Verdict:**

**PASS.**

#### 5.3.1.1.5 FCS\_DTLSC\_EXT.1.2 AGD

**Objective:**

- The evaluator shall ensure that the AGD describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE includes support for IP addresses, the evaluator shall ensure that the AGD provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.

**Evaluator Findings:**

- The evaluator ensured that the AGD describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE includes support for IP addresses, the evaluator ensured that the AGD provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.

The relevant information is found in the following section(s): **Subsection 9: Configuring a reference identifier for a trustpoint under section 10.1 Generating and Adding Certificates to a Certificate Manager**

Upon investigation, the evaluator found that the AGD states that: **The TOE supports reference identifiers using FQDN, IPv4 and IPv6 in the CN or SAN of the certificate.**

- **Configuring a reference identifier for a trustpoint**  
**sdwan\_client(cert-tp-mytrustpoint)# reference-id FQDN (FQDN or IPv4/IPv6)**  
**sdwan\_client(cert-tp-mytrustpoint)# validation identifier-check (strict/basic)**

**Note: “validation identifier-check” should always be set to “strict” in the Common Criteria configuration. The TOE supports both IPv4 and IPv6 as well as FQDN in the CN/SAN of a certificate. SAN always takes priority if it is present in the certificate.**

**Verdict:**

**PASS.**

#### 5.3.1.1.6 FCS\_DTLSC\_EXT.1.4 AGD

**Objective:**

- If the TSS indicates that the Supported Elliptic Curves/Supported Groups Extension must be configured to meet the requirement, the evaluator shall verify that the AGD includes configuration of the Supported Elliptic Curves/Supported Groups Extension.



#### Evaluator Findings:

- The evaluator checked the AGD Section **11.1.1. encryption-mode pki-DTLS** to determine if it includes the configuration for Supported Elliptic Curves/Supported Groups Extension.

The relevant information is found in **the NOTE of AGD Section 11.1.1. encryption-mode pki-DTLS**

Upon investigation, the evaluator found that the AGD states that: **The TOE does not support Elliptic Curves or Group Extensions.**

#### Verdict:

**PASS.**

#### 5.3.1.2 FCS\_DTLSS\_EXT.1 Extended: DTLS Server Protocol Without Mutual Authentication

##### 5.3.1.2.1 FCS\_DTLSS\_EXT.1.1 TSS

#### Objective:

- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified.
- The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

#### Evaluator Findings:

- The evaluator checked the description of the implementation of this protocol in the TSS Section and ensured that the ciphersuites supported are specified.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports DTLS 1.2 to allow two TOEs to be connected in a SD-WAN and supports both client and server.**

- The evaluator checked the TSS and ensured that the ciphersuites specified are identical to those listed for this component.

The relevant information is found in the following section(s): TOE Summary Specification **FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**

Upon investigation, the evaluator found that the TSS states that:

**The following ciphersuites are supported:**

- **TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA;**
- **TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA;**
- **TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256;**
- **TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256;**
- **TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256; and**
- **TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384**

#### Verdict:

**PASS.**

#### 5.3.1.2.2 FCS\_DTLSS\_EXT.1.3 TSS

##### Objective:

- The evaluator shall verify that the TSS describes how the DTLS Client IP address is validated prior to issuing a Server Hello message.

##### Evaluator Findings:

- The evaluator verified that the TSS describes how the DTLS Client IP address is validated prior to issuing a Server Hello message.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2.**

Upon investigation, the evaluator found that the TSS states that: **Upon receiving the client hello message, the TOE sends a hello verify request message and performs a stateless cookie exchange to ensure the DTLS client is not being spoofed. When certificates are exchanged the TOE will confirm that the FQDN, IPv4 or IPv6 identifier in the CN/SAN matches in the certificate. If the FQDN, IPv4 or IPv6 identifier in the CN/SAN doesn't match, the DTLS session will not be established.**Verdict:

PASS.

#### 5.3.1.2.3 FCS\_DTLSS\_EXT.1.4 TSS

##### Objective:

- If using ECDHE or DHE ciphers, the evaluator shall verify that the TSS describes the key agreement parameters of the server Key Exchange message.

##### Evaluator Findings:

- Upon investigation, the evaluator found that the ECHDE or DHE ciphers are not supported by TOE.

##### Verdict:

PASS.

#### 5.3.1.2.4 FCS\_DTLSS\_EXT.1.5 TSS

##### Objective:

- The evaluator shall verify that the TSS describes the actions that take place if a message received from the DTLS Client fails the MAC integrity check.

##### Evaluator Findings:

- The evaluator verified that the TSS Section describes the actions that take place if a message received from the DTLS Client fails the MAC integrity check.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **During internal channel communication between the client and server, if there is a message authentication code (MAC) verification failure, the TOE will silently discard the record and continue with the connection. Key establishment is performed using RSA with 2048 bits, 3072 bits, or 4096 bits.**

##### Verdict:

PASS.

#### 5.3.1.2.5 FCS\_DTLSS\_EXT.1.6 TSS

##### Objective:

- The evaluator shall verify that TSS describes how replay is detected and silently discarded for DTLS records that have previously been received and too old to fit in the sliding window.

##### Evaluator Findings:

- The evaluator verified that TSS describes how replay is detected and silently discarded for DTLS records that have previously been received and too old to fit in the sliding window.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **Valid record sequence numbers are maintained in a sliding window. For each record received, the TOE verifies if it is in the window boundary. Messages that are received where the same record was previously received or that are too old to fit in the sliding window are silently discarded.**

##### Verdict:

PASS.

#### 5.3.1.2.6 FCS\_DTLSS\_EXT.1.7 TSS[TD0569]

##### Objective:

- The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).
- If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS\_COP.1/DataEncryption.
- The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.
- If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in Section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.
- If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.

##### Evaluator Findings:

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_DTLSS\_EXT.1 & FCS\_DTLSS\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **The TOE does not support session resumption with either session ID's or session tickets.**

##### Verdict:

PASS.

#### 5.3.1.2.7 FCS\_DTLSS\_EXT.1.1 AGD

##### Objective:

- The evaluator shall also check the AGD to ensure that it contains instructions on configuring the TOE so that DTLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

##### Evaluator Findings:

- The evaluator also checked the AGD and ensured that it contains instructions on configuring the TOE so that DTLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

The relevant information is found in the following section(s): **11. SDWAN Encryption and encryption-mode**

Upon investigation, the evaluator found that the AGD activity states that:

**When the TOE is configured to be in a CC compliant configuration, DTLSv1.2 is the only accepted version of DTLS.**

**The only ciphers supported for this DTLS mode are the following:**

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288

##### Verdict:

PASS.

#### 5.3.1.2.8 FCS\_DTLSS\_EXT.1.4 AGD[TD0569]

##### Objective:

- The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD.

##### Evaluator Findings:

- The evaluator verified that any configuration necessary to meet the requirement must be contained in the AGD.

**The relevant information is found in) AGD Section 10 Introduction to Certificate Manager**

Upon investigation, the evaluator found that the AGD states that:

**The only ciphers supported for this DTLS mode are the following:**

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288

**NOTE: When the TOE is configured to be in a CC compliant configuration, DTLSv1.2 is the only accepted version of DTLS. Session ID's and session tickets are not supported in this configuration. No other configuration steps are necessary to operate in a CC compliant state.**

##### Verdict:

PASS.

#### 5.3.1.2.9 FCS\_DTLSS\_EXT.1.7 AGD

##### Objective:

- The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD.

##### Evaluator Findings:

- The evaluator verified that any configuration necessary to meet the requirement must be contained in the AGD.

The relevant information is found in the following section(s): **NOTE in Section 11.1.1 encryption-mode pki-DTLS**

Upon investigation, the evaluator found that the AGD states that: Session ID's and session tickets are not supported in this configuration.

##### Verdict:

PASS.

#### 5.3.1.3 FCS\_HTTPS\_EXT.1 HTTPS Protocol

##### 5.3.1.3.1 FCS\_HTTPS\_EXT.1 TSS

##### Objective:

- The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.

##### Evaluator Findings:

- The evaluator examined the TSS and determined that enough detail is provided to explain how the implementation complies with RFC 2818.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_HTTPS\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TSF uses the RFC 2818 HTTPS protocol for the that complies with RFC 2818. This protocol is used to provide a user with access to a virtual machines (VM) status if a VM is running on the TOE as well as viewing uptime, CPU usage and the time. Peer certificates are not required for authentication. This interface is only used for monitoring functionalities and is not used by an administrator to manage TSF data.**

##### Verdict:

PASS.

##### 5.3.1.3.2 FCS\_HTTPS\_EXT.1 AGD

##### Objective:

- The evaluator shall examine the AGD to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.

##### Evaluator Findings:

- The evaluator examined the AGD Section '**Services**' to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.

**The relevant information is found in the following section(s):AGD Section 4.1 Services**

Upon investigation, the evaluator found that the AGD states that:

## HTTPS

- In configuration mode, run following command:
  - (config)# ip http secure-server
- To specify the certificate the trustpoint uses for HTTPS, run the following command:
  - (config)# ip http secure-server certmgr <trustpoint>

**NOTE:** Session ID's are enabled by default for HTTPS when that service is turned on. No other configuration is necessary for HTTPS. The TOE only supports TLSv1.2 for all HTTPS connections. All other versions of TLS are rejected.

The HTTPS server on the TOE only supports the following algorithms using an RSA key size of 2048, 3072 or 4096 bits:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288

### Verdict:

PASS.

#### 5.3.1.4 FCS\_NTP\_EXT.1 NTP Protocol

##### 5.3.1.4.1 FCS\_NTP\_EXT.1.1 TSS

### Objective:

- The evaluator shall examine the TSS to ensure it identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained.
- The TOE must support at least one of the methods or may use multiple methods, as specified in the SFR element 1.2. the evaluator shall ensure that each method selected in the ST is described in the TSS, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp.

### Evaluator Findings:

- The evaluator examined the TSS Section to ensure it identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained.  
The relevant information is found in the following section(s): TOE Summary Specification 'FCS\_NTP\_EXT.1'  
Upon investigation, the evaluator found that the TSS states that: **The TOE uses NTP v3 (RFC 1305) and The NTP sources are defined by the Security Administrator.**
- The TOE must support at least one of the methods or may use multiple methods, as specified in the SFR element 1.2. the evaluator ensured that each method selected in the ST is described in the TSS, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp.  
The relevant information is found in the following section(s): TOE Summary Specification 'FCS\_NTP\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **NTP uses SHA1 for authenticating time stamps received. Upto three sources can be configured. NTPv3 is implemented on the TOE using Chrony version 3.4.**

**Verdict:**

**PASS.**

**5.3.1.4.2 FCS\_NTP\_EXT.1.1 AGD**

**Objective:**

- The evaluator shall examine the AGD to ensure it provides the Security Administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST.

**Evaluator Findings:**

- The evaluator examined the AGD to ensure it provides the Security Administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST.

The relevant information is found in the following section(s): **AGD Section 17. Configuring NTP**

Upon investigation, the evaluator found that the AGD states that:

- **Configure an NTP client in KlasOS with the following command in CONFIGURATION MODE**
  - **(conf)# ntp server <IP address>**
    - **IP address is the IP address of the NTP server.**

**Note: To configure multiple NTP servers, this command must be entered for every NTP server the administrator wants to sync to. The only version of NTP supported by the TOE is NTPv3.**

**Verdict:**

**PASS.**

**5.3.1.4.3 FCS\_NTP\_EXT.1.2 AGD**

**Objective:**

- For each of the secondary selections made in the ST, the evaluator shall examine the AGD to ensure it instructs the Security Administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp.

**Evaluator Findings:**

- The evaluator examined the AGD and ensured that, for each of the secondary selections made in the ST, it instructs the Security Administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp.

The relevant information is found in the following section(s) **AGD Section 17. Configuring NTP**

Upon investigation, the evaluator found that the AGD states that:

- **Client Authentication Key**
  - **If the NTP server supports cryptographic authentication using SHA-1, configure the correct key in KlasOS by appending a [key] option at the end of the ntp server command. In CONFIGURATION MODE:**

```
(conf)# ntp authenticate
(conf)# ntp authentication-key 1 sha1 <shared secret>
(conf)# ntp trusted-key 1
(conf)# ntp server <IP address> key 1
```

**Verdict:**

PASS.

5.3.1.4.4 FCS\_NTP\_EXT.1.3 AGD

**Objective:**

- The evaluator shall examine the AGD to ensure it provides the Security Administrator instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated.

**Evaluator Findings:**

- The evaluator examined the AGD Section '**Configuring NTP**' to ensure it provides the Security Administrator instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated.

The relevant information is found in the following section(s)AG**Section 17. Configuring NTP**

Upon investigation, the evaluator found that the AGD states that: **The TOE automatically denies any NTP timestamp updates from a multicast or broadcast IP address.**

**Verdict:**

PASS.

5.3.1.5 FCS\_SSHC\_EXT.1 SSH Client

5.3.1.5.1 FCS\_SSHC\_EXT.1.2 TSS[TD0636]

**Objective:**

- The evaluator shall check to ensure that the TSS contains a list of the public key algorithms that are acceptable for use for authentication and that this list is consistent with asymmetric key generation algorithms selected in FCS\_CKM.1, hashing algorithms selected in FCS\_COP.1/Hash, and signature generation algorithms selected in FCS\_COP.1/SigGen.
- The evaluator shall confirm the TSS is unambiguous in declaring the TOE's ability to authenticate itself to a remote endpoint with a user-based public key.
- If password-based authentication method has been selected in the FCS\_SSHC\_EXT.1.2, then the evaluator shall confirm it is also described in the TSS.

**Evaluator Findings:**

- The evaluator checked and ensured that the TSS Section contains a list of the public key algorithms that are acceptable for use for authentication and that this list is consistent with asymmetric key generation algorithms selected in FCS\_CKM.1, hashing algorithms selected in FCS\_COP.1/Hash, and signature generation algorithms selected in FCS\_COP.1/SigGen.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **SSH public key authentication is supported with the following key pairs: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384. The TOE supports the following RSA key sizes: 2048, 3072, and 4096.**



- The evaluator confirmed the TSS is unambiguous in declaring the TOE’s ability to authenticate itself to a remote endpoint with a user-based public key.  
The relevant information is found in the following section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**.

Upon investigation, the evaluator found that the TSS states that:

**Password based authentication is not supported by TOE.**

**Verdict:**

**PASS.**

**5.3.1.5.2 FCS\_SSHC\_EXT.1.3 TSS**

**Objective:**

- The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.

**Evaluator Findings:**

- The evaluator checked that the TSS Section ‘**FCS\_SSHC\_EXT.1**’ describes how “large packets” in terms of RFC 4253 are detected and handled.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **Packet sizes up to 33,292 bytes are accepted and packets exceeding this size are dropped and this event is logged by the TOE.**

**Verdict:**

**PASS.**

**5.3.1.5.3 FCS\_SSHC\_EXT.1.4 TSS**

**Objective:**

- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well.
- The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.

**Evaluator Findings:**

- The evaluator checked the description of the implementation of this protocol in the TSS Section ‘**FCS\_SSHC\_EXT.1**’ and ensured that optional characteristics are specified, and the encryption algorithms supported are specified as well.
- The evaluator checked the TSS Section ‘**FCS\_SSHC\_EXT.1**’ and ensured that the encryption algorithms specified are identical to those listed for this component.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports encryption algorithms AES-128-CBC, AES-256-CBC, AES-128-CTR and AES-256-CTR to ensure confidentiality of the session.**

**Verdict:**

**PASS.**

#### 5.3.1.5.4 FCS\_SSHC\_EXT.1.5 TSS[TD0636]

##### Objective:

- The evaluator shall confirm the TSS describes how a host-key public key (i.e., SSH server's public key) is associated with the server identity.
- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the host-key public key algorithms supported by the TOE are specified as well.
- The evaluator shall check the TSS to ensure that the host-key public key algorithms specified are identical to those listed for this component.
- If x509v3-based public key authentication algorithms are claimed, the evaluator shall confirm that the TSS includes the description of how the TOE establishes the server's identity and how this identity is confirmed with the one that is presented in the provided certificate. For example, the TOE could verify that a server's configured IP address matches the one presented in the server's x.509v3 certificate.

##### Evaluator Findings:

- The evaluator confirmed the TSS describes how a host-key public key (i.e., SSH server's public key) is associated with the server identity.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **An IP address is associated with each host-key public key when a key is uploaded to the TOE. The TOE identifies the public key that is presented by the server and verifies if it matches one of the stored keys within the client. If the presented key does not match, authentication is prevented.**

The evaluator checked the description of the implementation of this protocol in the TSS and ensured that optional characteristics are specified, and the host-key public key algorithms supported by the TOE are specified as well. The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

- Upon investigation, the evaluator found that the TSS states that: **SSH public key authentication is supported with the following key pairs: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384.**

- The evaluator checked the TSS and ensured that

- the host-key public key algorithms specified are identical to those listed for this component.

The relevant information is found in the following section(s): TOE Summary Specification '**FCS\_SSHC\_EXT.1**'

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the following hostkey algorithms: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384.**

- If x509v3-based public key authentication algorithms are claimed, the evaluator confirmed that the TSS includes the description of how the TOE establishes the server's identity and how this identity is confirmed with the one that is presented in the provided certificate.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **SSH password-based authentication and public key authentication are both supported with the following key pairs: ssh-rsa, ecdsa-s.ha2-nistp256, ecdsa-sha2-nistp384.**

- **X509v3 based public keys are not used by the TOE or claimed for SSH.**

##### Verdict:

PASS.



#### 5.3.1.5.5 FCS\_SSHC\_EXT.1.6 TSS

##### Objective:

- The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.

##### Evaluator Findings:

- The evaluator checked the TSS Section 'FCS\_SSHC\_EXT.1' and ensured that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the following data integrity algorithms: hmac-sha1, hmac-sha2-256, and hmac-sha2-512.**

##### Verdict:

PASS.

#### 5.3.1.5.6 FCS\_SSHC\_EXT.1.7 TSS

##### Objective:

- The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.

##### Evaluator Findings:

- The evaluator checked the TSS Section 'FCS\_SSHC\_EXT.1' and ensured that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the following key exchange algorithms: Diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384.**

##### Verdict:

PASS.

#### 5.3.1.5.7 FCS\_SSHC\_EXT.1.8 TSS

##### Objective:

- The evaluator shall check that the TSS specifies the following:
  - a. Both thresholds are checked by the TOE.
  - b. Rekeying is performed upon reaching the threshold that is hit first.

##### Evaluator Findings:

- The evaluator checked that the TSS Section 'FCS\_SSHC\_EXT.1' specifies the following:
  - a. Both thresholds are checked by the TOE.
  - b. Rekeying is performed upon reaching the threshold that is hit first.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHC\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE is capable of rekeying and verifies the following thresholds:**

- **No longer than one hour**
- **No more than 1 GB of transmitted data**

The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.

Verdict

PASS.

#### 5.3.1.5.8 FCS\_SSHC\_EXT.1.2 AGD[TD0636]

##### Objective:

- The evaluator shall check the AGD to ensure that it contains instructions to the administrator on how to ensure that only the allowed mechanisms are used in SSH connections initiated by the TOE.

##### Evaluator Findings:

- The evaluator checked the AGD to ensure that it contains instructions to the administrator on how to ensure that only the allowed mechanisms are used in SSH connections initiated by the TOE.

The relevant information is found in the following section(s): **9 SSH Tunnel for Trusted Channel**

Upon investigation, the evaluator found that the AGD states that:

**SSH client on the TOE is restricted to the following algorithms:**

- Encryption using AES-CTR-128, AES-CTR-256, AES-CBC-256 or AES-CBC-128
- Public key user and host authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384
- Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512
- Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.

**NOTE:** These algorithms are not configurable by an administrator. The algorithm used will depend on the algorithms the SSH server is using, and the type of key generated on the TOE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the TOE.

Verdict:

PASS.

#### 5.3.1.5.9 FCS\_SSHC\_EXT.1.4 AGD

##### Objective:

- The evaluator shall also check the AGD and ensured that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

##### Evaluator Findings:

- The evaluator also checked the AGD and ensured that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

The relevant information is found in the following section(s): **AGD Section 9 SSH Tunnel for Trusted Channel**

Upon investigation, the evaluator found that the AGD states that: **SSH client on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH client on the TOE is restricted to the following algorithms:**

- Encryption using AES-CBC-256 or AES-CBC-128

**Verdict:**

PASS.

5.3.1.5.10 FCS\_SSHC\_EXT.1.5 AGD

**Objective:**

- The evaluator shall also check the AGD to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

**Evaluator Findings:**

- The evaluator also checked the AGD to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

The relevant information is found in the following section(s): **9 SSH Tunnel for Trusted Channel**

Upon investigation, the evaluator found that the AGD states that: **SSH client on the TOE is restricted to the following algorithms:**

- Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384

**NOTE: These algorithms are not configurable by an administrator. The algorithm used will depend on the algorithms the SSH server is using and the type of key generated on the TOE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the TOE.**

**Verdict:**

PASS.

5.3.1.5.11 FCS\_SSHC\_EXT.1.6 AGD

**Objective:**

- The evaluator shall also check the AGD and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).

**Evaluator Findings:**

- The evaluator also checked the AGD and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).

The relevant information is found in the following section(s): **9 SSH Tunnel for Trusted Channel**

Upon investigation, the evaluator found that the AGD states that: **SSH client on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH client on the TOE is restricted to the following algorithms:**

- Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512

**NOTE: These algorithms are not configurable by an administrator. The algorithm used will depend on the algorithms the SSH server is using and the type of key generated on the TOE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the TOE.**

**Verdict:**

PASS.

5.3.1.5.12 FCS\_SSHC\_EXT.1.7 AGD

**Objective:**

- The evaluator shall also check the AGD to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

**Evaluator Findings:**

- The evaluator also checked the AGD Section '**SSH Tunnel for Trusted Channel**' and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

The relevant information is found in the following section(s) **9 SSH Tunnel for Trusted Channel**

Upon investigation, the evaluator found that the AGD states that: **SSH client on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH client on the ToE is restricted to the following algorithms:**

- **Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384**
- **Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.**

**NOTE: These algorithms are not configurable by an administrator. The algorithm used will depend on the algorithms the SSH server is using and the type of key generated on the ToE and is restricted to the algorithms outlined above. The use of any other cryptographic engines other than those listed above were not evaluated or tested during the CC evaluation of the TOE.**

**Verdict:**

PASS.

5.3.1.5.13 FCS\_SSHC\_EXT.1.8 AGD

**Objective:**

- If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the AGD describes how to configure those thresholds. Either the allowed values are specified in the AGD and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR.
- The evaluator shall check that the AGD describes that the TOE reacts to the first threshold reached.

**Evaluator Findings:**

- If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator checked that the AGD describes how to configure those thresholds. Either the allowed values are specified in the AGD and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR.

The relevant information is found in the following section(s): **9.3 Configure SSH Tunnel**

Upon investigation, the evaluator found that the AGD states that:

- The evaluator checked that the AGD Section '**Configure SSH Tunnel**' describes that the TOE reacts to the first threshold reached.

The relevant information is found in the following section(s): **9.3 Configure SSH Tunnel**

Upon investigation, the evaluator found that the AGD states that:

The ToE ensures that a SSH rekey happens after no more than 1 GB of data has been transmitted and received or after 1 hour, whichever is arrived at first. When a SSH rekey occurs the following message is displayed in the system log:

SSH Client Message:

```
2024-04-30T20:31:44.176220+00:00 KlasOS /usr/bin/ssh[2909]: %SYS-6-SSH_AUTH_REKEY: SSH rekey completed with x.x.x.xVerdict:
```

PASS.

5.3.1.6 FCS\_SSHS\_EXT.1 SSH Server

5.3.1.6.1 FCS\_SSHS\_EXT.1.2 TSS[TD0631]

Objective:

- The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS\_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).
- The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized\_keys file.
- If password-based authentication method has been selected in the FCS\_SSHS\_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.

Evaluator Findings:

- The evaluator checked and ensured that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS\_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).

The relevant information is found in the following section(s): TOE Summary Specification 'FCS\_SSHS\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **SSH password-based authentication and public key authentication are both supported with the following user and host key pairs: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384.**

- The evaluator confirmed that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized keys file.

The relevant information is found in the following section(s): TOE Summary Specification 'FCS\_SSHS\_EXT.1'

Upon investigation, the evaluator found that the TSS states that: **The TOE identifies the public key that is presented by the client and verifies if it matches one of the stored keys within the server. If the presented key does not match, authentication is prevented.**

- If password-based authentication method has been selected in the FCS\_SSHS\_EXT.1.2, then the evaluator confirmed its role in the authentication process is described in the TSS.

The relevant information is found in the following Section(s): TOE Summary Specification FCS\_SSHS\_EXT.1

Upon investigation, the evaluator found that the TSS states that:

**When a user logs into the TOE, they are authenticated via a username and password or public key. Password-based authentication is not required if a public key is being used. If public key authentication is not available, all users must log in using a password specified for that user account. The password is**

determined by the user and must conform to the requirements set out in FIA\_PMG\_EXT.1. When verifying a user's password, the one way hash is computed and the result is checked against the value stored for the username in the /etc/passwd file. Only certain programs on the TOE can access the /etc/passwd file, for example sshd. Users/admins do not have access.

**Verdict:**

PASS.

5.3.1.6.2 FCS\_SSHS\_EXT.1.3 TSS

**Objective:**

- The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.

**Evaluator Findings:**

- The evaluator checked that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_SSHS\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **Packet sizes up to 33,292 bytes are accepted and packets exceeding this size are dropped and this event is logged by the TOE.**

**Verdict:**

PASS.

5.3.1.6.3 FCS\_SSHS\_EXT.1.4 TSS

**Objective:**

- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well.
- The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.

**Evaluator Findings:**

- The evaluator checked the description of the implementation of this protocol in the TSS and ensured that optional characteristics are specified, and the encryption algorithms supported are specified as well.  
The relevant information is found in the following Section(s): TOE Summary Specification: **FCS\_SSHS\_EXT.1**  
Upon investigation, the evaluator found that the TSS states that: **. The TOE supports encryption algorithms.**
- The evaluator checked the TSS ensured that the encryption algorithms specified are identical to those listed for this component.

The relevant information is found in the following Section(s): TOE Summary Specification: **FCS\_SSHS\_EXT.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports encryption algorithms AES-128-CBC and AES-256-CBC to ensure confidentiality of the session.**

**Verdict:**

PASS.



#### 5.3.1.6.4 FCS\_SSHS\_EXT.1.5 TSS [TD0631]

##### Objective:

- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component.

##### Evaluator Findings:

- The evaluator checked the description of the implementation of this protocol in the TSS and ensured that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component.

The relevant information is found in the following section(s): TOE Summary Specification 'FCS\_SSHS\_EXT.1'.

Upon investigation, the evaluator found that the TSS states that: **SSH password-based authentication and public key authentication are both supported with the following user and host key pairs: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384.**

##### Verdict:

PASS.

#### 5.3.1.6.5 FCS\_SSHS\_EXT.1.6 TSS

##### Objective:

- The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms and that the list corresponds to the list in this component.

##### Evaluator Findings:

- The evaluator checked the TSS Section 'FCS\_SSHS\_EXT.1' and ensured that it lists the supported data integrity algorithms and that the list corresponds to the list in this component.

The relevant information is found in the following Section(s): TOE Summary Specification FCS\_SSHS\_EXT.1

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the following data integrity algorithms: hmac-sha1, hmac-sha2-256, and hmac-sha2-512 for SSH to ensure integrity of the session.**

##### Verdict:

PASS.

#### 5.3.1.6.6 FCS\_SSHS\_EXT.1.7 TSS

##### Objective:

- The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.

##### Evaluator Findings:

- The evaluator checked the TSS Section 'FCS\_SSHS\_EXT.1' and ensured that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.

The relevant information is found in the following Section(s): TOE Summary Specification FCS\_SSHS\_EXT.1

Upon investigation, the evaluator found that the TSS states that: **The supported key exchange algorithms are diffie-hellman-group14-sha1, ecdh-sha2-nistp256 and ecdh-sha2-nistp384.**

**Verdict:**

PASS.

5.3.1.6.7 FCS\_SSHS\_EXT.1.8 TSS

**Objective:**

- The evaluator shall check that the TSS specifies the following:
  - a. Both thresholds are checked by the TOE.
  - b. Rekeying is performed upon reaching the threshold that is hit first.

**Evaluator Findings:**

- The evaluator checked that the TSS Section 'FCS\_SSHS\_EXT.1' specifies the following:
  - a. Both thresholds are checked by the TOE.
  - b. Rekeying is performed upon reaching the threshold that is hit first.

The relevant information is found in the following Section(s): TOE Summary Specification FCS\_SSHS\_EXT.1

Upon investigation, the evaluator found that the TSS states that: **The TOE is capable of rekeying and verifies the following thresholds:**

- **No longer than one hour**
- **No more than 950 MB of transmitted data**

**The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.**

**Verdict**

PASS.

5.3.1.6.8 FCS\_SSHS\_EXT.1.4 AGD

**Objective:**

- The evaluator shall also check the AGD to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

**Evaluator Findings:**

- The evaluator also checked the AGD and ensured that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

**The relevant information is found in the following section(s) Section 7 Remote Administration Using SSH**

Upon investigation, the evaluator found that the AGD states that: **SSH server on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH server on the ToE is restricted to the following algorithms:**

- **Encryption using AES-CBC-256 or AES-CBC-128**
- **Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384**
- **Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512**
- **Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.**

**Verdict:**

PASS.

5.3.1.6.9 FCS\_SSHS\_EXT.1.5 AGD

**Objective:**

- The evaluator shall also check the AGD to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

**Evaluator Findings:**

- The evaluator also checked the AGD and ensured that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

The relevant information is found in the following section(s) :**7 Remote Administration Using SSH**

Upon investigation, the evaluator found that the AGD states that: **SSH server on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH server on the TOE is restricted to the following algorithms:**

- **Public key authentication using SSH-RSA, ECDSA-SHA2-NISTP256 or ECDSA-SHA2-NISTP384**

**Verdict:**

PASS.

5.3.1.6.10 FCS\_SSHS\_EXT.1.6 AGD

**Objective:**

- The evaluator shall also check the AGD to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).

**Evaluator Findings:**

- The evaluator also checked the AGD and ensured that and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).

The relevant information is found in the:**Section 7 Remote Administration Using SSH**

Upon investigation, the evaluator found that the AGD states that: **SSH server on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH server on the ToE is restricted to the following algorithms:**

- **Integrity using HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512**

**Verdict:**

PASS.

5.3.1.6.11 FCS\_SSHS\_EXT.1.7 AGD

**Objective:**

- The evaluator shall also check the AGD to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

#### Evaluator Findings:

- The evaluator also checked the AGD Section '**Remote Administration Using SSH**' and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

The relevant information is found in **Section 7 Remote Administration Using SSH**

Upon investigation, the evaluator found that the AGD states that: **SSH server on KlasOS supports SSH version 2 only. SSH version 1 is not supported.**

**SSH server on the ToE is restricted to the following algorithms:**

- **Key exchange using DIFFIE-HELLMAN-GROUP14-SHA1, ECDH over NIST P256 with SHA2 or ECDH over NIST P384 with SHA2.**

#### Verdict:

**PASS.**

5.3.1.6.12 FCS\_SSHS\_EXT.1.8 AGD

#### Objective:

- If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the AGD describes how to configure those thresholds. Either the allowed values are specified in the AGD and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR.
- The evaluator shall check that the AGD describes that the TOE reacts to the first threshold reached.

#### Evaluator Findings:

- If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator checked that the AGD describes how to configure those thresholds. Either the allowed values are specified in the AGD and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR.

The relevant information is found in the following section(s): **7.1 'Importing a Public Key'**

Upon investigation, the evaluator found that the AGD activity states that: **To import a public key into the ToE for SSH public key authentication by a remote administrator, first ensure a username is configured. See Section 3.1 Passwords on how to configure a username with password.**

**Once a username has been configured, type the following commands from global configuration mode:**

- **ip ssh pubkey-chain**
- **username <username>**
- **key-string <SSH public key>**

**The <SSH public key> is the full string taken from the SSH client PC public key file.**

**Once the public key is imported a user can SSH to the TOE without entering a password.**

- The evaluator checked that the AGD describes that the TOE reacts to the first threshold reached.

The relevant information is found in the following section(s): **7.1 'Importing a Public Key'**

Upon investigation, the evaluator found that the AGD states that:

**The ToE ensures that a SSH rekey happens after no more than 1 GB of data has been received or after 1 hour, whichever is arrived at first. When a SSH rekey occurs the following message is displayed in the system log:**

**SSH Client Message:**

2024-04-30T20:31:44.176220+00:00 KlasOS /usr/bin/ssh[2909]: %SYS-6-SSH\_AUTH\_REKEY: SSH rekey completed with x.x.x.x .

**Verdict:**

PASS.

5.3.1.7 FCS\_TLSS\_EXT.1 Extended: TLS Server Protocol Without Mutual Authentication

5.3.1.7.1 FCS\_TLSS\_EXT.1.1 TSS

**Objective:**

- The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified.
- The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

**Evaluator Findings:**

- The evaluator checked the description of the implementation of this protocol in the TSS Section 'ensured that the ciphersuites supported are specified.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_TLSS\_EXT.1.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the following TLS\_RSA ciphersuites using TLSv1.2**

- The evaluator checked the TSS Section 'and ensured that the ciphersuites specified are identical to those listed for this component.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_TLSS\_EXT.1.1**

Upon investigation, the evaluator found that the TSS states that: **The TOE supports the following TLS\_RSA ciphersuites using TLSv1.2:**

- *TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,*
- *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,*
- *TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,*
- *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,*
- *TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,*
- *TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288*

**Verdict:**

PASS.

5.3.1.7.2 FCS\_TLSS\_EXT.1.2 TSS

**Objective:**

- The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.

**Evaluator Findings:**

- The evaluator verified that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.

The relevant information is found in the following Section(s): TOE Summary Specification **FCS\_TLSS\_EXT.1**.

Upon investigation, the evaluator found that the TSS indicates that: **The TOE supports the TLS\_RSA ciphersuites specified in FCS\_TLSS\_EXT.1 using TLS 1.2. Connection attempts for older SSL and TLS versions will be rejected by the TOE.**

**Verdict:**

**PASS.**

**5.3.1.7.3 FCS\_TLSS\_EXT.1.3 TSS[TD0635]**

**Objective:**

- If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14.

**Evaluator Findings:**

- **The evaluator reviewed the ST and verified that the TOE does not claim ECDHE or DHE ciphers; hence, this assurance activity is not applicable.**

**Verdict:**

**PASS.**

**5.3.1.7.4 FCS\_TLSS\_EXT.1.4 TSS[TD0569]**

**Objective:**

- The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).
- If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS\_COP.1/DataEncryption.
- The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.
- If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in Section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.
- If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator shall verify that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.

**Evaluator Findings:**

- The evaluator verified that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).

The relevant information is found in the following section(s): TOE Summary Specification '**FCS\_TLSS\_EXT.1**.'

Upon investigation, the evaluator found that the TSS states that: **The TOE supports session resumption based on session IDs according to RFC 5246. Session resumption is based on a single context and operates according to the applicable RFCs.**

- The evaluator reviewed the ST and verified that the TOE does not supports session tickets.
- The evaluator verified that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). The TSS describes how session establishment and session resumption are always using a separate context and how the contexts interact with respect to session resumption (regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.

The relevant information is found in the following section(s): TOE Summary Specification 'FCS\_TLSS\_EXT.1.'

Upon investigation, the evaluator found that the TSS states that: **Sessions can be reused, provided all session properties and parameters are still valid. If there are any instances where properties are not valid anymore, they are implicitly rejected by the TOE and a full handshake will be performed.**

**Verdict:**

PASS.

5.3.1.7.5 FCS\_TLSS\_EXT.1.1 AGD

**Objective:**

- The evaluator shall check the AGD to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

**Evaluator Findings:**

- The evaluator checked the AGD and ensured that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

**The relevant information is found in the following section(s):AGD Section 4.1 Services**

Upon investigation, the evaluator found that the AGD states that:

- **HTTPS**
  - In configuration mode, run following command:
    - (config)# ip http secure-server
  - To specify the certificate the trustpoint uses for HTTPS, run the following command:
    - (config)# ip http secure-server certmgr <trustpoint>

**NOTE: Session IDs are enabled by default for HTTPS when that service is turned on. No other configuration is necessary for HTTPS. The TOE only supports TLSv1.2 for all HTTPS connections. All other versions of TLS are rejected. The HTTPS server on the TOE only supports the following algorithms using an RSA key size of 2048, 3072 or 4096 bits:**

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288

**Verdict:**

PASS.

#### 5.3.1.7.6 FCS\_TLSS\_EXT.1.2 AGD

##### Objective:

- The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD.

##### Evaluator Findings:

- The evaluator verified that any configuration necessary to meet the requirement must be contained in the AGD.

**The relevant information is found in the following section(s)AGD Section 4.1 Services**

Upon investigation, the evaluator found that the AGD states that: **The TOE only supports TLSv1.2 for all HTTPS connections. All other versions of TLS are rejected.**

##### Verdict:

PASS.

#### 5.3.1.7.7 FCS\_TLSS\_EXT.1.3 AGD

##### Objective:

- The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD.

##### Evaluator Findings:

- The evaluator verified that any configuration necessary to meet the requirement must be contained in the AGD.

**The relevant information is found in the following section(s)AGD Section 4.1 Services**

Upon investigation, the evaluator found that the AGD states that **The HTTPS server on the TOE only supports the following algorithms using an RSA key size of 2048, 3072 or 4096 bits:**

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288

##### Verdict:

PASS.

#### 5.3.1.7.8 FCS\_TLSS\_EXT.1.4 AGD[TD0569]

##### Objective:

- The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD.

##### Evaluator Findings:

- The evaluator verified that any configuration necessary to meet the requirement must be contained in the AGD.

**The relevant information is found in the following section(s)AGD Section 4.1 Services**

Upon investigation, the evaluator found that the AGD states that: **Session ID's are enabled by default for HTTPS when that service is turned on.**



**Verdict:**

**PASS.**

**5.3.2 Identification and Authentication (FIA)**

**5.3.2.1 FIA\_X509\_EXT.1/Rev X.509 Certificate Validation**

**5.3.2.1.1 FIA\_X509\_EXT.1/Rev TSS**

**Objective:**

- The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA\_X509\_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).
- The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS Section and explained in the AGD.

**Evaluator Findings:**

- The evaluator ensured the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA\_X509\_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).

The relevant information is found in the following section(s): TOE Summary Specification '**FIA\_X509\_EXT.1/Rev**'

Upon investigation, the evaluator found that the TSS states that: **The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.**

**Certificates are used to authenticate and establish secure SDWAN communication.**

**The TOE will check the validity of the DTLS Server certificate prior to establishing a secure DTLS connection. The certificate validation is determined based on reference ID verification, certificate path, extended key usage field, certificate expiry date, and the certificate revocation status.**

**The TOE also validates certificates in accordance with the following rules:**

- **RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.**
  - **The certification path must terminate with a trusted CA certificate designated as a trust anchor.**
  - **The TOE validates a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.**
- The TSS describes when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS Section and explained in the AGD.

The relevant information is found in the following Section(s): TOE Summary Specification **FIA\_X509\_EXT.1/Rev**

Upon investigation, the evaluator found that the TSS states that:

- The TOE validates the revocation status of the certificate using Online Certificate Status Protocol (OCSP) as specified in RFC 6960.
- The TOE validates the extendedKeyUsage field according to the following rules:
  - Server certificates presented for DTLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field
  - Client certificates presented for DTLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extended key usage field.

For an expired certificate, TOE will deny the connection.

During secure SDWAN connection establishment, any byte modification in the certificate will lead to connection failure.

The TOE used OCSP for revocation checking. If the validation of the certificate fails because the OCSP Server cannot be connected to it, the certificate shall not be accepted, and the connection is terminated. It verifies whether the certificate or intermediate CA certificate has been revoked when a leaf certificate is presented to the TOE as part of the certificate chain during authentication. Revocation checking is done during authentication on all certificates in

chain using OCSP. If only a leaf is presented to the TOE, that certificate will also be checked for its revocation status.

**Verdict:**

**PASS.**

*5.3.2.1.2 FIA\_X509\_EXT.1/Rev AGD*

**Objective:**

- The evaluator shall also ensure that the AGD describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA\_X509\_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.

**Evaluator Findings:**

- The evaluator also ensured that the AGD Section **11.1.1.1 'X509 Certificate Validation'** describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA\_X509\_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.

The relevant information is found in the following section(s): **AGD Section 11.1.1.1 X509 Certificate Validation**

Upon investigation, the evaluator found that the AGD states that:

- **X509 Certificate validation happens every DTLS connection attempt for both the server and client.**
- **DTLS connections always use mutual authentication.**
- **The following extendedKeyUsage fields are required in X509 certificates:**
  - **OCSP signing must be present in the OCSP signing certificate.**
  - **Server Authentication must be present in any DTLS server certificates.**
  - **Client Authentication must be present in any DTLS client certificates.**
- **OCSP is used for checking the revocation status of both leaf and intermediate certificates during DTLS connections**

- **Configure OCSP to be turned on using the following commands:**
  - `(config)#certmgr trustpoint <trustpoint>`
  - `(config)#validation revocation-check strict`

**Verdict:**

PASS.

5.3.2.2 FIA\_X509\_EXT.2 X.509 Certificate Authentication

5.3.2.2.1 FIA\_X509\_EXT.2 TSS

**Objective:**

- The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the AGD for configuring the operating environment so that the TOE can use the certificates.
- The evaluator shall examine the TSS and confirmed that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
- The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the AGD contains instructions on how this configuration action is performed.

**Evaluator Findings:**

- The evaluator checked the TSS and ensured that it describes how the TOE chooses which certificates to use, and any necessary instructions in the AGD for configuring the operating environment so that the TOE can use the certificates.

The relevant information is found in the following Section(s): TOE Summary Specification **FIA\_X509\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **Certificates to support DTLS can be configured from the CLI and SSH interfaces. If the TSF determines that the certificate is not valid when the DTLS channel is being setup, it will not accept the certificate.**

- The evaluator examined the TSS and confirmed that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel.

The relevant information is found in the following Section(s): TOE Summary Specification **FIA\_X509\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **If a connection cannot be established during the validity check of a certificate, the TOE will not accept the certificate and application data will not flow.**

- The evaluator verified that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator ensures that the AGD contains instructions on how this configuration action is performed.

The relevant information is found in the following Section(s): TOE Summary Specification **FIA\_X509\_EXT.2**

Upon investigation, the evaluator found that the TSS states that: **Certificates to support DTLS can be configured from the CLI and SSH interfaces. If the TSF determines that the certification is not valid when the DTLS channel is being setup it will not accept the certificate.**

**Verdict:**

PASS.

#### 5.3.2.2.2 FIA\_X509\_EXT.2 AGD

##### Objective:

- The evaluator shall also ensure that the AGD describes the configuration required in the operating environment so the TOE can use the certificates. The AGD shall also include any required configuration on the TOE to use the certificates. The AGD document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.

##### Evaluator Findings:

- The evaluator also ensured that the AGD describes the configuration required in the operating environment so the TOE can use the certificates. The AGD Section shall also includes any required configuration on the TOE to use the certificates. The AGD also describes the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.

The relevant information is found in the following **section(s): Section 4 Operational Environment, Section 10.1 Generating and Adding Certificates to a Certificate Manager and 10.2 Certificate Manager/Trustpoint Troubleshooting**

Upon investigation, the evaluator found that the AGD states that **the AGD provides instructions and warnings for configuring the operating environment so that the TOE can use the certificates.**

- **X509 Certificate validation happens every DTLS connection attempt for both the server and client.**
- **DTLS connections always use mutual authentication.**
- **The following extendedKeyUsage fields are required in X509 certificates:**
  - **OCSP signing must be present in the OCSP signing certificate.**
  - **Server Authentication must be present in any DTLS server certificates.**
  - **Client Authentication must be present in any DTLS client certificates.**
- **OCSP is used for checking the revocation status of certificates during DTLS connections.**
  - **Configure OCSP to be turned on using the following commands:**
    - **(config)#certmgr trustpoint <trustpoint>**
    - **(config)#validation revocation-check strict**

**NOTE: OCSP must be turned on when performing any DTLS connections using this device in order to be operated in a CC compliant state. OCSP checking is performed on all certificates in the presented chain. If a connection cannot be established to the OCSP server, the DTLS connection will be dropped, and the administrator will have to reattempt. No other configuration is needed to place the TOE in the proper operating environment to use the certificates.**

##### Verdict:

**PASS.**

#### 5.3.2.3 FIA\_X509\_EXT.3 Extended: X509 Certificate Requests

##### 5.3.2.3.1 FIA\_X509\_EXT.3 TSS

##### Objective:

- If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.

### Evaluator Findings:

- The evaluator verified that the TSS contains a description of the device-specific fields used in certificate requests.
- The relevant information is found in the following section(s): TOE Summary Specification 'FIA\_X509\_EXT.3'
- Upon investigation, the evaluator found that the TSS states that: **When generating a certificate request the TSF provides the public key and common name in the request. Device-specific information is not provided as part of the CSR.**

### Verdict:

PASS.

#### 5.3.2.3.2 FIA\_X509\_EXT.3 AGD

### Objective:

- The evaluator shall check to ensure that the AGD contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that the AGD includes instructions for establishing these fields before creating the Certification Request.

### Evaluator Findings:

- The evaluator checked and ensured that the AGD contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator ensured that the AGD includes instructions for establishing these fields before creating the Certification Request.

The relevant information is found in the following **section(s): Section 10.1 Generating and Adding Certificates to a Certificate Manager**

Upon investigation, the evaluator found that the AGD contains instructions on requesting certificates from a CA, including generation of a Certificate Request.

### Verdict:

PASS.

#### 5.3.3 Security Management (FMT)

##### 5.3.3.1 FMT\_MOF.1/Functions Management of Security Functions Behaviour TSS

### Objective:

- For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).

### Evaluator Findings:

- The evaluator examined the TSS and ensured that, for non-distributed TOEs, it details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).

The relevant information is found in the following Section(s): TOE Summary Specification **FMT\_MOF.1/Functions.**

Upon investigation, the evaluator found that the TSS states that: **The Security administrator can configure a SSH tunnel for secure transmission of audit data to a syslog server. The IP address of the system log and the port to be used can be configured.**

**Verdict:**

**PASS.**

5.3.3.2 FMT\_MOF.1/Functions AGD

**Objective:**

- For non-distributed TOEs, the evaluator shall also ensure the AGD describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.

**Evaluator Findings:**

- The evaluator examined the AGD and ensured that, for non-distributed TOEs, it describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.
- The relevant information is found in the: **Section 9 SSH Tunnel for Trusted Channel**
- Upon investigation, the evaluator found that the AGD states that:

**The ToE uses an SSH tunnel for the Trusted Channel for syslog messages that are sent from the ToE to a remote syslog server. Before configuring the tunnel on the ToE, copy the generated public key on the ToE to the syslog server authorized key file, normally located in /home/<user>/.ssh/authorized\_keys. If the file does not exist, it can be created.**

**Instructions on generating a keypair on the ToE are explained in Section 6.1. This is the same keypair used by the ToE SSH Server for the Host Key. The ToE ensures that a SSH rekey happens after no more than 1 GB of data has been transmitted and received or after 1 hour, whichever arrives at first. The SSH tunnel will attempt to reconnect automatically when it detects the connection to the remote SSH server is broken.**

**Verdict:**

**PASS.**

5.3.3.3 FMT\_MOF.1/Services Management of Security Functions Behaviour

5.3.3.3.1 FMT\_MOF.1/Services TSS

**Objective:**

- For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

**Evaluator Findings:**

- The evaluator examined the AGD and ensured that, for non-distributed TOEs, it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. The relevant information is found in the following section(s): TOE Summary Specification '**FMT\_MOF.1/Services**'  
Upon investigation, the evaluator found that the TSS states that:

**The TOE may be managed via the CLI (console and remote SSH). The specific services the administrator can start and stop and how they do it are shown below:**

- **SSH Administration**
  - Enabling and disabling remote SSH access can be done via the CLI
- **SSH syslog connections**
  - Enabling and disabling SSH syslog can be done via the CLI
- **SD-WAN Connections**
  - Enabling and disabling SD-WAN can be done via the CLI
- **HTTPS limited GUI**
  - Enabling and disabling the GUI can be done via the CLI

Local console and remote administration provide the same functionalities based on the level of authentication.

**Verdict:**

PASS.

5.3.3.3.2 FMT\_MOF.1/Services AGD

**Objective:**

- For non-distributed TOEs, the evaluator shall also ensure the AGD describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

**Evaluator Findings:**

- The evaluator examined the AGD and ensured that, for non-distributed TOEs, it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

The relevant information is found in the following Section(s): **Section 4.1 Services**

Upon investigation, the evaluator found that the AGD states that: The following ToE services can be started and stopped by an administrator:

- DNS server
  - Run the following command in Global Configuration mode to enable DNS:
    - **ip dns server**
  - Run the following command in Global Configuration mode to disable DNS:
    - **no ip dns server**
- NTP server
  - NTP Server is disabled by default and must remain disabled to be in a CC validated state.
  - The following command in Global Configuration mode will also disable NTP if it is found enabled:
    - **no ntp server <ntp server IP>**
- HTTPS
  - In configuration mode, run following command:
    - **(config)# ip http secure-server**
  - To specify the certificate the trustpoint uses for HTTPS, run the following command:
    - **(config)# ip http secure-server certmgr <trustpoint>**
- SSH Client
  - To get an SECSH formatted public key from the TOE, run the following command in privileged EXEC mode:
    - **show ip ssh**
- Remote Syslog



- To configure the logs to be sent to a syslog server, use the following command in global configuration mode:
  - **logging host 127.0.0.1**

**Verdict:**

**PASS.**

5.3.3.4 FMT\_MTD.1/CryptoKeys Management of TSF Data

5.3.3.4.1 FMT\_MTD.1/CryptoKeys TSS

**Objective:**

- For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.

**Evaluator Findings:**

- The evaluator examined the TSS Section '**FMT\_MTD.1/CryptoKeys**' and ensured that, for non-distributed TOEs, it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.

The relevant information is found in the following Section(s): TOE Summary Specification

**FMT\_MTD.1/CryptoKeys**

- Upon investigation, the evaluator found that the TSS states that: **The security administrator can generate, import, and delete cryptographic keys through the TOE's Global Configuration mode. The specific keys they can manage are listed below:**

**SSH public keys used for FCS\_SSHS\_EXT.1 and FCS\_SSHC\_EXT.1**

**X509 Public keys used for FCS\_DTLSS\_EXT.1 and FCS\_DTLSC\_EXT.1**

**Certificates used for DTLS connections**

**RSA keys used for HTTPS connections under FCS\_TLSS\_EXT.1**

**Verdict:**

**PASS.**

5.3.3.4.2 FMT\_MTD.1/CryptoKeys AGD

**Objective:**

- For non-distributed TOEs, the evaluator shall also ensure the AGD lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.

**Evaluator Findings:**

- The evaluator examined the AGD Section '**Cryptographic Key Generation**' and ensured that, for non-distributed TOEs, it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.

The relevant information is found in the following section(s): **AGD Section 6.1 Cryptographic Key Generation**

Upon investigation, the evaluator found that the AGD states that: **The TOE can support the generation of one (1) EC/RSA cryptographic keypair as follows in Common Criteria evaluated mode. This keypair is used by**



both the SSH Server on the TOE for the SSH Host Key (see Section 6.1.1 - SSH Host Key), and the SSH client on the TOE for establishing an SSH tunnel to a remote server (see Section 9 - SSH Tunnel for Trusted Channel):

- EC keys of size 256 or 384
- RSA keys of size 2048, 3072, or 4096

Before keys can be generated, a domain name must be configured on the TOE with the following command entered in global configuration mode:

- ip domain-name klas.cc.test

Each private key generated is stored on the system flash and each key can be zeroized securely as per Common Criteria requirements.

Generating, importing, modifying or zeroizing cryptographic keys is logged to the audit log. See Section 8 'Logging and Auditing' for information on the audit log and the format of the log messages. The audit log message for generating a crypto key would look like the following:

To generate an ECDSA keypair do the following in global configuration mode

- crypto key generate ec keysize <256|384> label <label name>

The <label name> is a unique identifier for the key.

#### RSA Keypair

To generate an RSA keypair do the following in global configuration mode:

- crypto key generate rsa general-keys modulus <2048|3072|4096> label <label name>

The <label name> is a unique identifier for the key.

Running the same command again with the same label name will overwrite the existing key with that label name.

The 'show crypto mypubkey all' command will display details of all existing keys on the TOE.

Note: The above keys can also be used for DTLS certificate generation. To learn more about how DTLS is used on the TOE, refer to sections 10 & 11

Further the AGD section '6.2 Cryptographic Key Zeroization' states the method to zeroize the keys:

Cryptographic keys can be zeroized using the following methods:

Using the crypto key zeroize command from global configuration mode:

- crypto key zeroize <rsa | ec>

Type 'crypto key zeroize' to zeroize all keypairs. Use the 'ec' option to just zeroize EC keypairs. Use the 'rsa' option to just zeroize RSA keys.

Generating a new key (See section 6.1.2 for ECDSA keys and section 6.1.3 for RSA keys) will overwrite and erase any existing keys.

The AGD 'Section 7.1 Importing a Public Key' states the information about Importing the keys:

To import a public key into the ToE for SSH public key authentication by a remote administrator, first ensure a username is configured. See section 3.1 Passwords on how to configure a username with password.

Once a username has been configured, type the following commands from global configuration mode:

- ip ssh pubkey-chain
- username <username>
- key-string <SSH public key>

The <SSH public key> is the full string taken from the SSH client PC public key file.

Once the public key is imported a user can SSH to the ToE without entering a password

**Verdict:**

PASS.

## 6 Security Assurance Requirements

### 6.1 TOE Summary Specification (ASE\_TSS.1)

#### 6.1.1 ASE\_TSS.1.1C

**Objective:**

- The evaluator shall examine the TSS to determine that it is clear which TOE components contribute to each SFR or how the TSFI that is identified as being security relevant.
- The evaluator shall verify the sufficiency to fulfil the related SFRs. This includes checking that the TOE as a whole fully covers all SFRs and that all functionality that is required to be audited is in fact audited regardless of the component that carries it out.

**Evaluator Findings:**

- The evaluator examined the TSS to determine that it is clear which TOE components contribute to each SFR or how the TSFI that is identified as being security relevant.
- The evaluator verified the sufficiency to fulfil the related SFRs. This includes checking that the TOE as a whole fully covers all SFRs and that all functionality that is required to be audited is in fact audited regardless of the component that carries it out.

**Verdict:**

PASS.

### 6.2 Basic Functional Specification (ADV\_FSP)

#### 6.2.1 ADV\_FSP.1

##### 6.2.1.1 ADV\_FSP.1-1

**Objective:**

- The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.

**Evaluator Findings:**

- The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the AGD Evaluation Activities.

**Verdict:**

PASS.

##### 6.2.1.2 ADV\_FSP.1-2

**Objective:**

- The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.

**Evaluator Findings:**

- The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each AGD Activity is associated with a specific SFR. The Evaluation Findings for each AGD Activity identify the relevant interfaces, thus providing a mapping.

**Verdict:**

PASS.

6.2.1.3 ADV\_FSP.1-3

**Objective:**

- The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.

**Evaluator Findings:**

- The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the AGD Activities.

**Verdict:**

PASS.

6.2.1.4 ADV\_FSP.1-5

**Objective:**

- The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

**Evaluator Findings:**

- The evaluator examined the interface documentation to develop a mapping of the interfaces to SFRs.

**Verdict:**

PASS.

### 6.3 Operational User Guidance (AGD\_OPE)

6.3.1 AGD\_OPE.1

6.3.1.1 AGD\_OPE.1-1

**Objective:**

- The evaluator shall ensure the AGD is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

**Evaluator Findings:**

- The evaluator checked the requirements below are met by the AGD. The AGD is distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on [www.niap-ccevs.org](http://www.niap-ccevs.org).

**Verdict:**

PASS.

### 6.3.1.2 AGD\_OPE.1-2

#### Objective:

- The evaluator shall ensure that the AGD is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.

#### Evaluator Findings:

- The evaluator ensured that the AGD is provided for every Operational Environment that the product supports as claimed in the Security Target. Section 1.3 titled **Supported hardware and Software** of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are:

TOE Model	Specifications
VoyagerVMm (i3) and VoyagerVMm (i5)	5 <sup>th</sup> Gen Intel® Dual Core i3-5010U (1.8 GHz) Broadwell-U, 8 GB DDR3 RAM
	5 <sup>th</sup> Gen Intel® Quad Core i5-5350U (1.8 GHz) Broadwell-U, 32 GB DDR3 RAM
TRX R2 (4-core) and TRX R2 (8 core)	Atom™/Denverton C3508 Intel® Atom™ Denverton C3508 4-Core processor with 1.6 GHz clock. 8 GB RAM (upgradeable to 32 GB)
	Atom™/Denverton C3708 Intel® Atom™ Denverton C3708 4-Core processor with 1.7 GHz clock. 8 GB RAM (upgradeable to 32 GB)
VoyagerVM 3.0	Xeon D-1539 Intel® Xeon Processor D1539 16-Core with 48 or 96 GB RAM
	Xeon D-1559 Intel® Xeon Processor D1559 12-Core with 48 or 96 GB RAM
	Xeon D-1577 Intel® Xeon Processor D1577 16-Core with 48 or 96 GB RAM

The following software version is the Common Criteria validated software:

- KlasOS Keel 5.4.0

#### Verdict:

**PASS.**

### 6.3.1.3 AGD\_OPE.1-3

#### Objective:

- The evaluator shall ensure that the AGD contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

#### Evaluator Findings:

- The evaluator ensured that the AGD contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the AGD Activities for the cryptographic SFRs, the evaluator ensured that the AGD contains the necessary instructions for configuring the cryptographic engines.

**Verdict:**

PASS.

6.3.1.4 AGD\_OPE.1-4

**Objective:**

- The evaluator shall ensure the AGD makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.

**Evaluator Findings:**

- The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the Section titled **1.4 Operational Environment** specifies features that are not assessed and tested by the EAs. The evaluator ensured the AGD makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.

**Klas Voyager Keel device provides the following features which are outside the scope of the NIAP Common Criteria validation:**

- **SNMP**
- **Spanning-Tree**
- **Port Security**
- **TACACS+**
- **RADIUS**

**The section titled ‘1.3 Supported Hardware and Software’ specifies the validated software version:**

- **KlasOS Keel 5.4.0**

**Verdict:**

PASS.

6.3.1.5 AGD\_OPE.1-5[TD0536]

**Objective:**

- In addition, the evaluator shall ensure that the following requirements are also met:
  - The AGD shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
  - **[TD0536]** The AGD must describe the process for verifying updates to the TOE for each method selected for FPT\_TUD\_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps:
    - Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).
    - Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature.
  - The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The AGD shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.

### Evaluator Findings:

- The evaluator verified the AGD contains instructions for configuring any cryptographic engines in AGD\_OPE.1 Test #3.
- The evaluator verified the AGD describes the process for verifying updates in FPT\_TUD\_EXT.1 AGD 2.
- The evaluator verified the AGD makes it clear which security functionality is covered by the Evaluation Activities in AGD\_OPE.1 Test #4.

### Verdict:

PASS.

## 6.4 Preparative Procedures (AGD\_PRE)

### 6.4.1 AGD\_PRE.1

#### 6.4.1.1 AGD\_PRE.1-1

#### Objective:

- The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).

#### Evaluator Findings:

- The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the Sections titled **8.4 Sending Logs to Syslog Server** and **9 SSH Tunnel for Trusted Channel** of the AGD. The evaluator found that these Sections describe how the Operational Environment must meet:
  - **OE.ADMIN\_CREDENTIALS\_SECURE**
  - **OE.NO\_GENERAL\_PURPOSE**
  - **OE.NO\_THRU\_TRAFFIC\_PROTECTION**
  - **OE.PHYSICAL**
  - **OE.RESIDUAL\_INFORMATION**
  - **OE.TRUSTED\_ADMN**
  - **OE.UPDATES**

#### Verdict:

PASS.

#### 6.4.1.2 AGD\_PRE.1-2

#### Objective:

- The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.

#### Evaluator Findings:

- The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the AGD **Section 1.4 Operational Environment** describes each of the devices in the operating environment, including,
  - **Syslog Server**
  - **Local Console**
  - **Management workstation with SSH client**
  - **NTP Server**

The Section titled **1.3 Supported Hardware and Software** of AGD identifies the following supported platform:

- **VoyagerVMm (i3) and VoyagerVMm (i5)**
- **TRX R2 (4-core) and TRX R2 (8 core)**
- **VoyagerVM 3.0**

#### Verdict:

**PASS.**

6.4.1.3 AGD\_PRE.1-3

#### Objective:

- The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.

#### Evaluator Findings:

- The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including:
  - **Syslog Server**
  - **Local Console**
  - **Management workstation with SSH client**
  - **NTP Server**

#### Verdict:

**PASS.**

6.4.1.4 AGD\_PRE.1-4

#### Objective:

- The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.

#### Evaluator Findings:

- The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD\_PRE.1 Test #3.

#### Verdict:

**PASS.**



#### 6.4.1.5 AGD\_PRE.1-5

##### **Objective:**

- In addition, the evaluator shall ensure that the following requirements are also met. The preparative procedures must:
  - include instructions to provide a protected administrative capability; and
  - identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.

##### **Evaluator Findings:**

- The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The Sections titled **3 User Identification and Authentication** were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH for remote administration.

##### **Verdict:**

PASS.

### 6.5 Assurance Activities (ALC)

#### 6.5.1 ALC\_CMC.1

##### **Objective:**

- When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.

##### **Evaluator Findings:**

- The evaluator verified that the ST, TOE and AGD are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.

##### **Verdict:**

PASS.

#### 6.5.2 ALC\_CMS.1

##### **Objective:**

- When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.

##### **Evaluator Findings:**

- The evaluator verified that the ST, TOE and AGD are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.

##### **Verdict:**

PASS.

## 6.6 Independent Testing – Conformance (ATE\_IND)

### 6.6.1 ATE\_IND.1

#### Objective:

- The evaluator performs the CEM work units associated with the ATE\_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.

#### Evaluator Findings:

- The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE\_IND.1 in the CEM and in the SFR-related Evaluation Activities.

#### Verdict:

PASS.

## 6.7 Vulnerability Survey (AVA\_VAN)

### 6.7.1 AVA\_VAN.1

#### 6.7.1.1 AVA\_VAN.1-1[TD0547]

#### Objective:

- In addition to the activities specified by the CEM in accordance with Table 2, the evaluator shall perform the following activities.

*The evaluator shall examine the documentation outlined below provided by the developer to confirm that it contains all required information. This documentation is in addition to the documentation already required to be supplied in response to the EAs listed previously.*

The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components should identify at a minimum the processors used by the TOE. Software components include applications, the operating system and other major components that are independently identifiable and reusable (outside of the TOE), for example a web server, protocol or cryptographic libraries, (independently identifiable and reusable components are not limited to the list provided in the example). This additional documentation is merely a list of the name and version number of the components and will be used by the evaluators in formulating vulnerability hypotheses during their analysis.

If the TOE is a distributed TOE then the developer shall provide:

- a. documentation describing the allocation of requirements between distributed TOE components as in [NDcPP, 3.4]
- b. a mapping of the auditable events recorded by each distributed TOE component as in [NDcPP, 6.3.3]
- c. additional information in the Preparative Procedures as identified in the refinement of AGD\_PRE.1 in additional information in the Preparative Procedures as identified in 3.4.1.2 and 3.5.1.2.

### Evaluator Findings:

The evaluator collected this information from the developer which was used to feed into the Public Domain Search. Refer to evaluator findings in section 6.7.1.2 below. The TOE is not a distributed TOE.

### Verdict:

PASS.

#### 6.7.1.2 AVA\_VAN.1-2

### Objective:

- The evaluator formulates hypotheses in accordance with process defined in Appendix A. The evaluator documents the flaw hypotheses generated for the TOE in the report in accordance with the guidelines in Appendix A.3. The evaluator shall perform vulnerability analysis in accordance with Appendix A.2. The results of the analysis shall be documented in the report according to Appendix A.3.

### Evaluator Findings:

- The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of publicly available information are provided below.
  - <https://nvd.nist.gov/vuln/search>
  - <https://www.cvedetails.com/vulnerability-search.php>
  - <http://www.kb.cert.org/vuls/html/search>
  - [www.exploitsearch.net](http://www.exploitsearch.net)
  - [www.securiteam.com](http://www.securiteam.com)
  - <http://nessus.org/plugins/index.php?view=search>
  - <http://www.zerodayinitiative.com/advisories>
  - <https://www.exploit-db.com/>
  - <https://www.rapid7.com/db/vulnerabilities>
- The vulnerability searches were performed on March 12, 2024, April 23, 2024, June 7, 2024, and final search June 17, 2024. No open vulnerabilities applicable to the TOE were identified.
- The evaluator examined public domain vulnerability searches by performing a keyword and CPE search. The terms used for this search were based on the vendor's name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:
  - (OpenSSH 9.3p2) cpe:/:openbsd:openssh:9.3
  - (OpenSSL 3.0.8) cpe:/:openssl:openssl:3.0.8
  - (GNU C Library 2.31) cpe:2.3:a:glibc:glibc:2.31
  - (Linux-PAM 1.3.1) cpe:2.3:a:linux-pam:linux-pam:1.3.1:.....\*
  - (rsyslogd 8.34.0) cpe:/:rsyslog:rsyslog:8.34.0
  - (chronyd 3.4) cpe:/:chrony\_project:chrony:3.4
  - (KlasOS Keel v5.4.0)
  - (Klas Voyager VMm)
  - (Klas Voyager VM3)
  - (Klas TRXr2)

- The evaluation lab examined each result provided from NVD and Tenable search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.

**Verdict:**

PASS.

## 7 Detailed Test Cases (Test Activities)

### 7.1 Auth

#### 7.1.1 FAU\_STG.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall access the audit trail without authentication as Security Administrator (either by authentication as a nonadministrative user, if supported, or without authentication at all) and attempt to modify and delete the audit records. The evaluator shall verify that these attempts fail.</p> <p>According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to access the audit trail can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• The evaluator creates a non-administrative user on the TOE.</li><li>• The evaluator logs in as the non-administrative user on the TOE.</li><li>• The evaluator would attempt to modify logs as non-administrative user.</li></ul>
<b>Expected Test Results</b>	The TOE should not allow the modification of audit logs.
<b>Pass/Fail with Explanation</b>	Pass, The TOE prevents the non-administrative user from being able to modify or delete log files.
<b>Result</b>	Pass

#### 7.1.2 FAU\_STG.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall access the audit trail as an authorized administrator and attempt to delete the audit records. The evaluator shall verify that these attempts succeed. The evaluator shall verify that only the records authorized for deletion are deleted.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• The evaluator logs in as the administrative user.</li><li>• The evaluator attempts to access logs on the TOE.</li><li>• The evaluator attempts to delete logs on the TOE.</li></ul>
<b>Expected Test Results</b>	The administrative user will successfully be able to access and delete logs on the TOE.
<b>Pass/Fail with Explanation</b>	Pass, the TOE allows an administrator to access and delete logs.
<b>Result</b>	Pass

### 7.1.3 FIA\_AFL.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):</p> <p>Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure account lockout.</li> <li>• Try to connect to the TOE with wrong credentials two consecutive times to lockout the account.</li> <li>• Login with correct credentials and verify that it is not successful.</li> <li>• Verify with logs.</li> </ul>
<b>Expected Test Results</b>	The maximum number of successive unsuccessful attempts can be configured on the TOE. The TOE does not allow for access to the device even with correct credentials after an account fails authentication successively for the configured maximum number of unsuccessful attempts.
<b>Pass/Fail with Explanation</b>	Pass. The TOE did not allow to access after using incorrect credentials three times even when using correct credentials. This meets the testing requirements.
<b>Result</b>	Pass

### 7.1.4 FIA\_AFL.1 Test #2a

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):</p> <p>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:</p> <p>If the <b>administrator action</b> selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator unlocks the locked admin account.</li> <li>• The evaluator documents successful login after lockout with timestamps.</li> </ul>
<b>Expected Test Results</b>	The user will be able to successfully login once the account isn't locked out anymore.
<b>Pass/Fail with Explanation</b>	Pass, The test passes after a successful login after being locked out and a timestamp.

<b>Result</b>	Pass
---------------	------

### 7.1.5 FIA\_AFL.1 Test #2b

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):</p> <p>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:</p> <p>If the <b>time period</b> selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorisation attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorisation attempt using valid credentials results in successful access.</p>
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to time period not being selected.

### 7.1.6 FIA\_PMG\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator configures password management to be composed of the following criteria. <ul style="list-style-type: none"> <li>○ A combination of upper and lower case letters, numbers, and the special characters</li> <li>○ Minimum password length shall be configurable to 15 characters</li> </ul> </li> <li>• The evaluator documents password management policy success with log evidence.</li> <li>• The evaluator attempts to create 3 users (good11, good22, good33) that meet the password requirements. <ul style="list-style-type: none"> <li>○ Username good11 secret G00dpassword11!</li> <li>○ Username good22 secret G00dpassword22!</li> <li>○ Username: good33 secret G00dpassword33!</li> </ul> </li> <li>• The evaluator tries to establish a TOE connection using all above 3 users that meet the password requirements. <ul style="list-style-type: none"> <li>○ Connection attempt for user good11</li> <li>○ Connection attempt for user good22</li> <li>○ Connection attempt for user good33</li> </ul> </li> </ul>

<b>Expected Test Results</b>	The password management will be configured to include special characters and have a minimum password length of 15 characters.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows successful connections once the users have been created due to the password configuration meeting the password requirements.
<b>Result</b>	Pass

### 7.1.7 FIA\_PMG\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
<b>Test Steps</b>	The evaluator attempts to create 3 users (bad4, bad5, bad6) that do not meet the password requirements. <ul style="list-style-type: none"> <li>• Username bad11 secret BAD12345^&amp;*()</li> <li>• Username bad22 secret 123\$%^Bad</li> <li>• Username bad33 secret 1234567890bad</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow the creation of a password that does not have special characters, upper- and lower-case letters.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow users to be created that do not meet the password requirements.
<b>Result</b>	Pass

### 7.1.8 FIA\_UIA\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:  Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
<b>Test Steps</b>	Local <ul style="list-style-type: none"> <li>• The evaluator configures local authentication.</li> <li>• The evaluator shows log evidence of the configuration.</li> <li>• The evaluator attempts a successful connection.</li> <li>• The evaluator displays an unsuccessful connection attempt.</li> </ul> Remote <ul style="list-style-type: none"> <li>• The evaluator attempts a successful connection.</li> </ul>



	<ul style="list-style-type: none"> <li>• The evaluator shows log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> <li>• The evaluator displays an unsuccessful connection attempt.</li> <li>• The evaluator shows log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul> <p>Remote Public Key</p> <ul style="list-style-type: none"> <li>• The evaluator configures the TOE for a public key connection.</li> <li>• The evaluator displays a successful connection attempt.</li> <li>• The evaluator shows log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> <li>• Remove the public key from TOE to facilitate unsuccessful connection</li> <li>• The evaluator displays an unsuccessful connection attempt</li> <li>• The evaluator shows log evidence of the connection attempt</li> <li>• The evaluator shows packet capture evidence of the connection attempt</li> </ul>
<b>Expected Test Results</b>	The TOE should allow a successful connection with correct login information. The TOE should not allow the evaluator to successfully authenticate with incorrect login information.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful login and rejects the login appropriately with incorrect credentials for both local and remote interfaces.
<b>Result</b>	Pass

### 7.1.9 FIA\_UIA\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:</p> <p>Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator configures the login banner.</li> <li>• The evaluator authenticates to the TOE remotely and demonstrates the login banner displays properly.</li> <li>• The evaluator authenticates to the TOE locally and demonstrates the login banner displays properly.</li> <li>• The evaluator authenticates to the TOE using public key authentication and demonstrates the login banner displays properly.</li> <li>• The evaluator demonstrates the TOE properly responds to ICMP requests</li> </ul>
<b>Expected Test Results</b>	The TOE will be configured to show that the login banner will be available prior to login. The TOE will also respond to ICMP requests.

<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully displays the configured login banner and responds to ICMP requests for both remote and local login methods.
<b>Result</b>	Pass

#### 7.1.10 FIA\_UIA\_EXT.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:  Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>The evaluator attempts a connection to the TOE using the local console.</li> <li>The evaluator verifies that the only option presented is a login prompt and a banner.</li> </ul>
<b>Expected Test Results</b>	The local TOE interface appropriately displays the banner prior to logging in to the TOE.
<b>Pass/Fail with Explanation</b>	Pass, The TOE appropriately offers the correct services prior to logging in.
<b>Result</b>	Pass

#### 7.1.11 FIA\_UIA\_EXT.1 Test #4

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:  Test 4: For distributed TOEs where not all TOE components support the authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2, the evaluator shall test that the components authenticate Security Administrators as described in the TSS.
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not being distributed.

#### 7.1.12 FIA\_UAU.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following test for each method of local login allowed:  The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>The evaluator attempts a connection to the local console.</li> </ul>

	<ul style="list-style-type: none"> <li>The evaluator provides authentication logs showing the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should obscure the password information on the console authentication attempt.
<b>Pass/Fail with Explanation</b>	Pass, The TOE obscures password information on the local authentication attempt.
<b>Result</b>	Pass

### 7.1.13 FMT\_MOF.1/AutoUpdate Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable automatic checking for updates or automatic updates (whichever is supported by the TOE) without prior authentication as Security Administrator (by authenticating as a user with no administrator privileges or without user authentication). The attempt to enable/disable automatic checking for updates should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable automatic checking for updates can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not supporting automatic checking of updates.

### 7.1.14 FMT\_MOF.1/AutoUpdate Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable automatic checking for updates or automatic updates (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable automatic checking for updates should be successful.
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not supporting automatic checking of updates.

### 7.1.15 FMT\_MOF.1/ManualUpdate Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
<b>Test Steps</b>	<p>Local</p> <ul style="list-style-type: none"> <li>The evaluator logs in as a non-administrative user.</li> <li>The evaluator attempts to update a setting on the TOE.</li> </ul>

	<p>HTTPS</p> <ul style="list-style-type: none"> <li>• The evaluator logs in as a non-administrative user.</li> <li>• The evaluator attempts to update a setting on the TOE.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow an update to the TOE without proper authorization.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow a non-administrative user to update an image.
<b>Result</b>	Pass

#### 7.1.16 FMT\_MOF.1/ManualUpdate Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
<b>Pass/Fail with Explanation</b>	Pass, This test has been exercised with FPT_TUD_EXT.1 Test#1.
<b>Result</b>	Pass

#### 7.1.17 FMT\_MOF.1/Functions (1) Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1 (if '<b>transmission of audit data to external IT entity</b>' is selected from the second selection together with '<b>modify the behaviour of</b>' in the first selection): The evaluator shall try to modify all security related parameters for</p> <p>configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.</p>
<b>Test Steps</b>	<p>Local</p> <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator attempts privilege escalation on the TOE.</li> <li>• The evaluator attempts to modify logging settings.</li> <li>• The evaluator document evidence of the command attempts and the connection.</li> </ul> <p>HTTPS</p>

	<ul style="list-style-type: none"> <li>• The evaluator logs in as a non-administrative user.</li> <li>• The evaluator attempts to modify logging settings on the TOE.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow modification of settings without the proper permissions.
<b>Pass/Fail with Explanation</b>	Pass, The user was unable to successfully modify the syslog server settings.
<b>Result</b>	Pass

### 7.1.18 FMT\_MOF.1/Functions (1)Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 (if 'transmission of audit data to external IT entity' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed.</p> <p>The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.</p>
<b>Test Steps</b>	<p>Local</p> <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator attempts privilege escalation on the TOE.</li> <li>• The evaluator attempts to modify logging settings.</li> <li>• The evaluator document evidence of the command attempts and the connection.</li> </ul> <p>HTTPS</p> <ul style="list-style-type: none"> <li>• The evaluator logs in as a non-administrative user.</li> <li>• The evaluator attempts to modify logging settings on the TOE.</li> </ul>
<b>Expected Test Results</b>	The modification of the logging settings to an external syslog server will be successful.
<b>Pass/Fail with Explanation</b>	Pass, The test passes with proper evidence that the TOE was successfully configured for an external logging host.
<b>Result</b>	Pass

### 7.1.19 FMT\_MOF.1/Functions (2) Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1 (if ' <b>handling of audit data</b> ' is selected from the second selection together with ' <b>modify the behaviour of</b> ' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not selecting the options in the ST

### 7.1.20 FMT\_MOF.1/Functions (2) Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2 (if ' <b>handling of audit data</b> ' is selected from the second selection together with ' <b>modify the behaviour of</b> ' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.  The evaluator does not necessarily have to test all possible values of the security related parameters for configuration of the handling of audit data but at least one allowed value per parameter.
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not selecting the options in the ST

### 7.1.21 FMT\_MOF.1/Functions (3) Test #1

Item	Data
<b>Test Assurance Activity</b>	(if ' <b>audit functionality when Local Audit Storage Space is full</b> ' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This attempt should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.

<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not selecting the options in the ST
-----------------------------------	------------------------------------------------------------------------------------

### 7.1.22 FMT\_MOF.1/Functions (3) Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>(if 'audit functionality when Local Audit Storage Space is full' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full with prior authentication as Security Administrator. This attempt should be successful. The effect of the change shall be verified.</p> <p>The evaluator does not necessarily have to test all possible values for the behaviour when Local Audit Storage Space is full but at least one change between allowed values for the behaviour</p>
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not selecting the options in the ST

### 7.1.23 FMT\_MOF.1/Functions Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>(if in the first selection '<b>determine the behaviour of</b>' has been chosen together with for any of the options in the second selection):</p> <p>The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall fail.</p> <p>According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.</p>
<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not selecting the options in the ST

### 7.1.24 FMT\_MOF.1/Functions Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>(if in the first selection '<b>determine the behaviour of</b>' has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection with prior authentication as Security Administrator. This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions with Security Administrator authentication shall be successful.</p>

<b>Pass/Fail with Explanation</b>	N/A This test is not applicable due to the TOE not selecting the options in the ST
-----------------------------------	------------------------------------------------------------------------------------

### 7.1.25 FMT\_MOF.1/Services Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable this service/these services can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
<b>Test Steps</b>	Local <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the TOE as a standard user.</li> <li>• The evaluator attempts to modify a service on the TOE.</li> </ul> HTTPS <ul style="list-style-type: none"> <li>• The evaluator logs in as a non-administrative user.</li> <li>• The evaluator attempts to update a setting on the TOE.</li> </ul>
<b>Expected Test Results</b>	The TOE will deny the service starting due to lack of permissions.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow modification of services from a standard user on either the local or HTTPS interface.
<b>Result</b>	Pass

### 7.1.26 FMT\_MOF.1/Services Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
<b>Test Steps</b>	Local <ul style="list-style-type: none"> <li>• The evaluator attempts a login to the TOE as an administrative user.</li> <li>• The evaluator attempts to modify a service on the TOE.</li> </ul> HTTPS <ul style="list-style-type: none"> <li>• The evaluator logs in as a non-administrative user.</li> <li>• The evaluator attempts to update a setting on the TOE.</li> </ul>



<b>Expected Test Results</b>	The TOE will allow a service to be started since the administrative user has the proper permissions to execute the command at the local interface. The same administrative user is not allowed to perform any administrative actions on the HTTPS interface due to limited functionality.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows modification of services from an administrative user from a local interface but not the HTTPS interface.
<b>Result</b>	Pass

### 7.1.27 FMT\_MTD.1/CryptoKeys Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the TOE as a standard user.</li> <li>• The evaluator attempts to generate a cryptographic key.</li> <li>• The evaluator documents the failure of the cryptographic key generation.</li> </ul>
<b>Expected Test Results</b>	The TOE will demonstrate the inability to generate a cryptographic key due to lack of permissions from the non-admin user.
<b>Pass/Fail with Explanation</b>	Pass, The test passes because the cryptographic key was not able to be generated due to the lack of permissions of the non-admin user.

### 7.1.28 FMT\_MTD.1/CryptoKeys Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the TOE as an administrative user.</li> <li>• The evaluator attempts to generate a cryptographic key.</li> <li>• The evaluator documents the success of the cryptographic key generation.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow the user to generate a cryptographic key.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows an administrative user to generate a cryptographic key successfully.
<b>Result</b>	Pass

### 7.1.29 FMT\_SMF.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator tests management functions as part of testing the SFRs identified in Section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
<b>Test Output</b>	<p><b>FMT_SMF.1.1</b></p> <p><b>The TSF shall be capable of performing the following management functions:</b></p> <ul style="list-style-type: none"> <li>• <b><i>Ability to administer the TOE locally and remotely;</i></b>  <i>Exercised in FTA_SSL_EXT.1.1 test 1</i></li>   <li>• <b><i>Ability to configure the access banner;</i></b>  <i>Exercised in FTA_TAB.1</i></li>   <li>• <b><i>Ability to configure the session inactivity time before session termination or locking;</i></b>  <i>Exercised in FTA_SSL_EXT.1.1 test 1</i></li>   <li>• <b><i>Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;</i></b>  <i>Exercised in FPT_TUD_EXT.1 Test 1</i></li>   <li>• <b><i>Ability to configure the authentication failure parameters for FIA_AFL.1;</i></b>  <i>Exercised in FIA_AFL.1 test 1 and 2b</i> <ul style="list-style-type: none"> <li>○ <b><i>Ability to start and stop services;</i></b>  <i>Exercised in FMT_MOF.1/Services test 1 and 2</i></li>   <li>○ <b><i>Ability to modify the behaviour of the transmission of audit data to an external IT entity;</i></b>  <i>Exercised in FAU_STG_EXT.1 test 1.</i></li>   <li>○ <b><i>Ability to manage the cryptographic keys;</i></b>  <i>Exercised in FIA_X509_EXT.1.1/Rev test 1a, 1b, and 2</i></li>   <li>○ <b><i>Ability to configure the cryptographic functionality;</i></b>  <i>Exercised in FIA_X509_EXT.1.1/Rev test 1a and 1b</i></li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ <b><u>Ability to re-enable an Administrator account;</u></b> Exercised in FIA_AFL.1 test 1</li> <li>○ <b><u>Ability to set the time which is used for time-stamps;</u></b> Exercised in FCS_NTP_EXT.1.1</li> <li>○ <b><u>Ability to configure NTP;</u></b> Exercised in FCS_NTP_EXT.1.1 Test #1</li> <li>○ <b><u>Ability to configure the reference identifier for the peer;</u></b> Exercised in FCS_DTLSC_EXT.1.2 test 1 and 2</li> <li>○ <b><u>Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;</u></b> Exercised in FIA_X509_EXT.1.1/Rev test 3</li> <li>○ <b><u>Ability to import X.509v3 certificates to the TOE's trust store;</u></b> Exercised in FIA_X509_EXT.1.1/Rev test 8a, 8b, and 8c</li> <li>○ <b><u>Ability to manage the trusted public keys database;</u></b> Exercised in FCS_SSHS_EXT.1.5 test 1 and 2.</li> <li>○ <b><u>No other capabilities].</u></b></li> </ul>
<b>Pass/Fail with Explanation</b>	Pass, FMT_SMF.1 Specification of Management Functions requirements has been met throughout the various security functionality testing of the TOE.
<b>Result</b>	Pass

### 7.1.30 FMT\_SMR.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.

<b>Pass/Fail with Explanation</b>	<p><b>FMT_SMR.2.1</b></p> <p>The TSF shall maintain the roles:</p> <ul style="list-style-type: none"> <li>• <i>Security Administrator</i></li> </ul> <p>This test has been exercised in FIA_UIA_EXT.1 and FTA_SSL.3.</p> <p><b>FMT_SMR.2.2</b></p> <p>The TSF shall be able to associate users with roles.</p> <p>This test has been exercised in FAU_STG_EXT.1 test 2.</p> <p><b>FMT_SMR.2.3</b></p> <p>The TSF shall ensure that the conditions</p> <ul style="list-style-type: none"> <li>• <i>The Security Administrator role shall be able to administer the TOE locally;</i></li> </ul> <p>This test has been exercised by FIA_AFL.1 test 1.</p> <ul style="list-style-type: none"> <li>• <i>The Security Administrator role shall be able to administer the TOE remotely;</i></li> </ul> <p>This test has been exercised by FMT_MOF.1/Functions(1) test 2 are satisfied.</p>
<b>Result</b>	Pass

### 7.1.31 FTA\_SSL.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator configures a remote SSH timeout period of 1 minute on administrative sessions.</li> <li>• The evaluator shows log evidence of the timeout being configured.</li> <li>• The evaluator tests the idle timeout of the SSH session.</li> <li>• The evaluator shows log evidence of the session timing out.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator configures a remote SSH timeout period of 2 minutes on administrative sessions.</li> <li>• The evaluator tests the idle timeout of the SSH session.</li> <li>• The evaluator shows log evidence of the session timing out.</li> </ul>

<b>Expected Test Results</b>	The TOE will act as configured with idle timeouts getting observed.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully times out the remote session after being configured to 1 minute and 2 minutes.
<b>Result</b>	Pass

### 7.1.32 FTA\_SSL.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the local console.</li> <li>• The evaluator displays logs of the connection attempt.</li> <li>• The evaluator terminates the session.</li> <li>• The evaluator displays logs of the connection termination.</li> </ul>
<b>Expected Test Results</b>	The logs for the TOE will show a successful login and logout.
<b>Pass/Fail with Explanation</b>	Pass, The test passes, the evaluator was able to successfully login to the local console of the TOE and logout. The logs reflected these actions accurately.
<b>Result</b>	Pass

### 7.1.33 FTA\_SSL.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a remote connection as an administrative user.</li> <li>• The evaluator displays logs of the connection attempt.</li> <li>• The evaluator terminates the connection.</li> <li>• The evaluator displays logs of the connection termination.</li> <li>• The evaluator displays packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE will accurately reflect the login and log off in the system logs.

<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful login and is able to terminate the session.
<b>Result</b>	Pass

#### 7.1.34 FTA\_SSL\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
<b>Test Steps</b>	<p>Local Login</p> <ul style="list-style-type: none"> <li>• The evaluator configures a local console timeout period of 1 minute on administrative sessions.</li> <li>• The evaluator shows log evidence of the timeout being configured.</li> <li>• The evaluator attempts a connection to the TOE and tests the idle timeout of the console session.</li> <li>• The evaluator shows log evidence of the session timing out after 1 minute.</li> <li>• The evaluator configures a local console timeout period of 2 minutes on administrative sessions.</li> <li>• The evaluator shows log evidence of the timeout being configured.</li> <li>• The evaluator attempts a connection to the TOE and tests the idle timeout of the console session.</li> <li>• The evaluator shows log evidence of the session timing out after 2 minutes.</li> </ul>
<b>Expected Test Results</b>	The TOE will act as configured with the timeouts for the local console.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully times out the evaluator after the allotted periods of time.
<b>Result</b>	Pass

#### 7.1.35 FTA\_TAB.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.

<b>Test Steps</b>	As specified in the TSS, the TOE can be accessed through serial console (Local) or remotely connecting to the TOE through SSHv2. Local (Serial Console): <ul style="list-style-type: none"> <li>• The evaluator configures the access banners on TOE.</li> <li>• The evaluator authenticates to the TOE.</li> <li>• The evaluator documents the configuration steps.</li> </ul> Remote (SSHv2): <ul style="list-style-type: none"> <li>• The evaluator configures the access banners on TOE.</li> <li>• The evaluator authenticates to the TOE.</li> <li>• The evaluator documents the configuration steps.</li> </ul>
<b>Expected Test Results</b>	The TOE should react as configured displaying the newly configured login banner for each method of access (Local and Remote).
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully displays the login banner for each method of access (Local and Remote) after the user authenticates.
<b>Result</b>	Pass

### 7.1.36 FTP\_TRP.1/Admin Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
<b>Test Steps</b>	SSH <ul style="list-style-type: none"> <li>• The evaluator attempts a connection with the TOE.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator displays packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE will get configured for each different key in the key exchange and will successfully create a session for each login.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful SSH connection.
<b>Result</b>	Pass

### 7.1.37 FTP\_TRP.1/Admin Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
<b>Pass/Fail with Explanation</b>	Pass, this test has been exercised in FTP_TRP.1/Admin Test #1.
<b>Result</b>	Pass

## 7.2 Audit

### 7.2.1 FAU\_GEN.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&amp;A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.</p> <p>Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Trigger each auditable event on the TOE.</li> <li>• Verify that each audit record is generated and contains the required information.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE is able to generate audit records for each of the events described in the ST under the FAU_GEN.1.1 along with the events mentioned in Table 13 of the ST.</li> <li>• The TOE is able to generate audit records for establishment and termination of a channel for SSH and HTTPS.</li> <li>• The audit records generated match the proper format as specified in the guidance documentation</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. TOE generates the audit records for the auditable events listed in the table. This meets the testing requirements.
<b>Result</b>	Pass

### 7.2.2 FAU\_GEN.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of auditable events to TOE components in the Security Target. For all events involving more than one TOE component when an audit event is triggered, the evaluator has to check that the event has been audited on both sides (e.g. failure of building up a secure communication channel between the two components). This is not limited to error cases but includes also events about successful actions like successful build up/tear down of a secure communication channel between TOE components.</p>
<b>Pass/Fail with Explanation</b>	N/A. The TOE is not distributed.



### 7.2.3 FAU\_STG\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator confirms the name and version of the audit server.</li> <li>• The evaluator configures the TOE to use the syslog server.</li> <li>• The evaluator generates audit records.</li> <li>• The evaluator verifies via packet capture that syslog messages have been sent encrypted.</li> </ul>
<b>Expected Test Results</b>	The TOE will be successfully configured to the audit server, and the audit records will successfully be recorded on the audit server.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully sends encrypted audit logs to the syslog server.
<b>Result</b>	Pass

### 7.2.4 FAU\_STG\_EXT.1 Test #2 (a)

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option ' <b>drop new audit data</b> ' in FAU_STG_EXT.1.3).
<b>Pass/Fail with Explanation</b>	N/A Drop new audit data is not selected in the ST. This test is not applicable.

### 7.2.5 FAU\_STG\_EXT.1 Test #2 (b)

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option ' <b>overwrite previous audit records</b> ' in FAU_STG_EXT.1.3)

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator reconfigures the TOE logging to local.</li> <li>• The evaluator generates audit records until the log buffer is full.</li> <li>• The evaluator highlights the oldest timestamp in the local audit log.</li> <li>• The evaluator verifies the oldest message gets changed to the new messages as new audit logs are written.</li> </ul>
<b>Expected Test Results</b>	The test will pass as the TOE overwrites previous audit records with a new audit log buffer.
<b>Pass/Fail with Explanation</b>	Pass, the test passes as the oldest audit logs are overwritten by the newer audit logs, as the existing buffer gets deleted, and a new buffer gets created.
<b>Result</b>	Pass

### 7.2.6 FAU\_STG\_EXT.1 Test #2 (c)

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The TOE behaves as specified (for the option ' <b>other action</b> ' in FAU_STG_EXT.1.3).
<b>Pass/Fail with Explanation</b>	N/A Other action is not selected in the ST. This test is not applicable.

### 7.2.7 FAU\_STG\_EXT.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3: If the TOE complies with FAU_STG_EXT.2/LocSpace the evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.2/LocSpace are correct when performing the tests for FAU_STG_EXT.1.3
<b>Pass/Fail with Explanation</b>	N/A FAU_STG_EXT.2/LocSpace is not selected in the ST.

### 7.2.8 FAU\_STG\_EXT.1 Test #4

Item	Data
<b>Test Assurance Activity</b>	Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.
<b>Pass/Fail with Explanation</b>	N/A The TOE is not distributed. This test is not applicable.

### 7.2.9 FAU\_STG\_EXT.2/LocSpace

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.2/LocSpace are correct when performing the tests for FAU_STG_EXT.1.3.</p> <p>For distributed TOEs the evaluator shall verify the correct implementation of counting of lost audit data for all TOE components that are supporting this feature according to the description in the TSS.</p>
<b>Pass/Fail with Explanation</b>	N/A FAU_STG_EXT.2/LocSpace is not selected in the ST, also the TOE is not distributed. This test is not applicable.

### 7.2.10 FAU\_STG\_EXT.3/LocSpace Test#1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall verify that a warning is issued by the TOE before the local storage space for audit data is full.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• The evaluator copies a large file to the TOE.</li><li>• The evaluator displays audit logging.</li></ul>
<b>Expected Test Results</b>	The TOE should display the warning message showing that the audit log is nearing full.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully displays a warning message for the local storage space.
<b>Result</b>	Pass

### 7.2.11 FAU\_STG\_EXT.3/LocSpace Test#2

Item	Data
<b>Test Assurance Activity</b>	For distributed TOEs the evaluator shall verify the correct implementation of display warning for local storage space for all TOE components that are supporting this feature according to the description in the TSS. The evaluator shall verify that each component that supports this feature according to the description in the TSS is capable of generating a warning itself or through another component.
<b>Pass/Fail with Explanation</b>	N/A. The TOE is not distributed.

### 7.2.12 FCS\_NTP\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The version of NTP selected in element 1.1 and specified in the ST shall be verified by observing establishment of a connection to an external NTP server known to be using the specified version(s) of NTP.</p> <p>This may be combined with tests of other aspects of FCS_NTP_EXT.1 as described below.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• The evaluator configures the connection to an existing NTP server.</li><li>• The evaluator documents evidence of the NTP synchronizing.</li></ul>

<b>Expected Test Results</b>	Evidence confirming that the TOE has successfully synchronized with an external NTP server, using the NTP version selected in element 1.1 and specified in the ST.
<b>Pass/Fail with Explanation</b>	Pass, The test passes as the TOE is successfully able to synchronize the time with the NTP server using the NTP version selected in element 1.1 and specified in the ST.
<b>Result</b>	Pass

### 7.2.13 FCS\_NTP\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	[Conditional] If the <b>message digest algorithm</b> is claimed in element 1.2, the evaluator will change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source. The evaluator shall use a packet sniffer to capture the network traffic between the TOE and the NTP server. The evaluator uses the captured network traffic, to verify the NTP version, to observe time change of the TOE and uses the TOE's audit log to determine that the TOE accepted the NTP server's timestamp update. The captured traffic is also used to verify that the appropriate message digest algorithm was used to authenticate the time source and/or the appropriate protocol was used to ensure integrity of the timestamp that was transmitted in the NTP packets.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator displays the current time on the TOE.</li> <li>• The evaluator configures the TOE with an incorrect sha1 algorithm not recognized by the TOE.</li> <li>• The evaluator shows that the NTP synchronize is not successful.</li> <li>• The evaluator configures the TOE with a correct sha1 algorithm that is recognized by the TOE.</li> <li>• The evaluator shows the NTP synchronize is successful.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow a successful and unsuccessful NTP synchronize.
<b>Pass/Fail with Explanation</b>	Pass, The TOE syncs with the NTP Server when the supported message-digest algorithm is configured and does not sync when an unsupported message digest algorithm is used, this meets testing requirements.
<b>Result</b>	Pass

### 7.2.14 FCS\_NTP\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure NTP server(s) to support periodic time updates to broadcast and multicast addresses. The evaluator shall confirm the TOE is configured to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. The evaluator shall check that the time stamp is not updated after receipt of the broadcast and multicast packets.
<b>Test Steps</b>	<p>Broadcast:</p> <ul style="list-style-type: none"> <li>• The evaluator configures the NTP server to support periodic time updates to broadcast addresses.</li> <li>• The evaluator configures the TOE to not accept broadcast and multicast NTP packets.</li> <li>• The evaluator synchronizes time on the TOE and verify that it fails.</li> </ul> <p>Multicast:</p> <ul style="list-style-type: none"> <li>• The evaluator configures the NTP server to support periodic time updates to multicast addresses.</li> </ul>

	<ul style="list-style-type: none"> <li>• The evaluator configures the TOE to not accept broadcast and multicast NTP packets.</li> <li>• The evaluator to synchronize time on the TOE and verify that it fails.</li> </ul>
<b>Expected Test Results</b>	TOE time stamp should not be updated after receipt of broadcast and multicast packets from NTP server.
<b>Pass/Fail with Explanation</b>	Pass, the TOE appropriately rejects any time updates from a broadcast or multicast NTP packets.
<b>Result</b>	Pass

### 7.2.15 FCS\_NTP\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is updated after receipt of the NTP packets. The purpose of this test to verify that the TOE can be configured to synchronize with multiple NTP servers. It is up to the evaluator to determine that the multi-source update of the time information is appropriate and consistent with the behaviour prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4. <b>TD0528 has been applied.</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure three different NTP servers on the TOE.</li> <li>• Verify the NTP servers being configured.</li> <li>• Manually change the time of the TOE.</li> <li>• Verify the NTP packets being exchanged between the TOE and the first NTP server.</li> <li>• Verify the timestamp being updated after syncing with the first NTP server.</li> <li>• Stop the NTP service on the first NTP server to make it unreachable.</li> <li>• Manually change the time of the TOE.</li> <li>• Verify the NTP packets being exchanged between the TOE and the second NTP server.</li> <li>• Verify the timestamp being updated after syncing with the second NTP server.</li> <li>• Stop the NTP service on the second NTP server to make it unreachable.</li> <li>• Manually change the time of the TOE.</li> <li>• Verify the NTP packets being exchanged between the TOE and the third NTP server.</li> <li>• Verify the timestamp being updated after syncing with the third NTP server.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support the configuration of three NTP servers.</li> <li>• When three NTP servers are configured on the TOE, the TOE should successfully synchronize with all the NTP servers.</li> <li>• Packet captures should show NTP packets are received from each of the NTP servers.</li> <li>• TOE logs should show the addition of NTP servers and time synchronization with them for NTP version 3.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to successfully sync its time with multiple configured NTP servers.
<b>Result</b>	Pass

### 7.2.16 FCS\_NTP\_EXT.1.4 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers).</p> <p>The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system time. This rogue time source needs to be configured in a way (e.g. degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behaviour of a correctly-functioning NTP server.</p> <p><b>TD0528 has been applied.</b></p>
Test Steps	<ul style="list-style-type: none"> <li>• The evaluator displays current time on TOE.</li> <li>• The evaluator configures the NTP server on the TOE and synchronizes it with the TOE.</li> <li>• The evaluator displays packet capture evidence of a successful sync.</li> <li>• The evaluator displays log evidence of a successful sync.</li> <li>• The evaluator configures a different NTP server on the TOE and synchronizes it with the TOE.</li> <li>• The evaluator displays packet capture evidence of a successful sync.</li> <li>• The evaluator displays log evidence of a successful sync.</li> <li>• The evaluator replays the packets from the first sync to the TOE.</li> <li>• The evaluator verifies that the TOE does not sync from the packet replay.</li> </ul>
Expected Test Results	The TOE should not successfully sync from the packets being replayed.
Pass/Fail with Explanation	Pass. The TOE successfully rejects the unsolicited time sync.
Result	Pass

### 7.2.17 FPT\_STM\_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: If the TOE supports direct <b>setting of the time by the Security Administrator</b> then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Steps	<ul style="list-style-type: none"> <li>• The evaluator configures the time on the TOE.</li> <li>• The evaluator shows log evidence of the time being set.</li> <li>• The evaluator displays the current time.</li> </ul>
Expected Test Results	The TOE has the ability to have the time set and will do so successfully.
Pass/Fail with Explanation	Pass. The test passes as the user was successfully sets the system time on the device.
Result	Pass

### 7.2.18 FPT\_STM\_EXT.1 Test #2

Item	Data
Test Assurance Activity	Test 2: If the TOE supports the <b>use of an NTP server</b> ; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Pass/Fail with Explanation	Pass. Test has been exercised in FCS_NTP_EXT.1.1 Test#1 and FCS_NTP_EXT.1.2 Test#1.
Result	Pass

### 7.2.19 FPT\_STM\_EXT.1 Test #3

Item	Data
Test Assurance Activity	Test 3: [conditional] If the TOE obtains time from the underlying VS, the evaluator shall record the time on the TOE, modify the time on the underlying VS, and verify the modified time is reflected by the TOE. If there is a delay between the setting the time on the VS and when the time is reflected on the TOE, the evaluator shall ensure this delay is consistent with the TSS and Guidance. <b>TD0632 has been applied.</b>
Pass/Fail with Explanation	N/A The TOE is not a virtual network device.

### 7.2.20 FTP\_ITC.1 Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Pass/Fail with Explanation	Pass, Test has been exercised in FAU_STG_EXT.1 Test#1.
Result	Pass

### 7.2.21 FTP\_ITC.1 Test #2

Item	Data
Test Assurance Activity	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
Pass/Fail with Explanation	Pass, Test has been exercised in FAU_STG_EXT.1 Test#1.
Result	Pass

### 7.2.22 FTP\_ITC.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Pass/Fail with Explanation	Pass, Test has been exercised in FAU_STG_EXT.1 Test#1.
Result	Pass

### 7.2.23 FTP\_ITC.1 Test #4

Item	Data
Test Assurance Activity	<p>Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.</p> <p>The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations:</p> <ol style="list-style-type: none"> <li>1. A duration that exceeds the TOE's application layer timeout setting,</li> <li>2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer.</li> </ol> <p>The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.</p> <p>In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.</p>
Test Steps	<p><b>Less than application layer timeout test (5 seconds)</b></p> <p><b>Syslog</b></p> <ul style="list-style-type: none"> <li>• The evaluator authenticates to the TOE.</li> <li>• The evaluator displays log evidence of a successful login.</li> <li>• The evaluator displays packet capture data between the TOE and syslog server.</li> </ul> <p><b>Greater than application layer timeout test (30 seconds)</b></p> <p><b>Syslog</b></p> <ul style="list-style-type: none"> <li>• The evaluator authenticates to the TOE.</li> <li>• The evaluator displays log evidence of a successful login.</li> <li>• The evaluator displays packet capture data between the TOE and syslog server.</li> </ul> <p><b>Note: The network interruption between the TOE and testing VM was caused by a network switch in between the TOE and main network switch. The network cable was unplugged from the network switch and not the TOE.</b></p>
Expected Test Results	The TOE should successfully send encrypted data after network interruptions for both durations.
Pass/Fail with Explanation	Pass, The TOE successfully starts encrypted data again after connectivity gets interrupted.
Result	Pass



## 7.3 Crypto

### 7.3.1 FCS\_CKM.1 RSA

Item	Data
<b>Test Assurance Activity</b>	<p>Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported).</p> <p>Key Generation for FIPS PUB 186-4 RSA Schemes The evaluator shall verify the implementation of RSA Key Generation by the TOE using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent e, the private prime factors p and q, the public modulus n and the calculation of the private signature exponent d.</p> <p>Key Pair generation specifies 5 ways (or methods) to generate the primes p and q. These include: Random Primes: Provable primes Probable primes Primes with Conditions: Primes p1, p2, q1, q2, p and q shall all be provable primes Primes p1, p2, q1, and q2 shall be provable primes and p and q shall be probable primes Primes p1, p2, q1, q2, p and q shall all be probable primes</p> <p>To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: RSA KeyGen Key size / Modulus: 2048 CAVP #: A4573 Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

### 7.3.2 FCS\_CKM.1 ECC

Item	Data
<b>Test Assurance Activity</b>	<p>Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported).</p>

	<p>Key Generation for Elliptic Curve Cryptography (ECC)  FIPS 186-4 ECC Key Generation Test  For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall require the implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator shall submit the generated key pairs to the public key verification (PKV) function of a known good implementation.</p> <p>FIPS 186-4 Public Key Verification (PKV) Test  For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator shall obtain in response a set of 10 PASS/FAIL values.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: ECDSA KeyGen, ECDSA KeyVer  Curves: P-256, P-384, P-521  CAVP #: A4573  Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

### 7.3.3 FCS\_CKM.1 FFC

Item	Data
<b>Test Assurance Activity</b>	<p>Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported).</p> <p>Key Generation for Finite-Field Cryptography (FFC)  The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime <math>p</math>, the cryptographic prime <math>q</math> (dividing <math>p-1</math>), the cryptographic group generator <math>g</math>, and the calculation of the private key <math>x</math> and public key <math>y</math>.</p> <p>The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime <math>q</math> and the field prime <math>p</math>:</p> <ul style="list-style-type: none"> <li>• Primes <math>q</math> and <math>p</math> shall both be provable primes</li> <li>• Primes <math>q</math> and field prime <math>p</math> shall both be probable primes</li> </ul> <p>and two ways to generate the cryptographic group generator <math>g</math>:</p> <ul style="list-style-type: none"> <li>• Generator <math>g</math> constructed through a verifiable process</li> <li>• Generator <math>g</math> constructed through an unverifiable process.</li> </ul> <p>The Key generation specifies 2 ways to generate the private key <math>x</math>:</p> <ul style="list-style-type: none"> <li>• <math>\text{len}(q)</math> bit output of RBG where <math>1 \leq x \leq q-1</math></li> <li>• <math>\text{len}(q) + 64</math> bit output of RBG, followed by a mod <math>q-1</math> operation and a <math>+1</math> operation, where <math>1 \leq x \leq q-1</math>.</li> </ul>

	<p>The security strength of the RBG must be at least that of the security offered by the FFC parameter set.</p> <p>To test the cryptographic and field prime generation method for the provable primes method and/or the group generator <math>g</math> for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set.</p> <p>For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm</p> <ul style="list-style-type: none"> <li>• <math>g \neq 0,1</math></li> <li>• <math>q</math> divides <math>p-1</math></li> <li>• <math>g^q \bmod p = 1</math></li> <li>• <math>g^x \bmod p = y</math></li> </ul> <p>for each FFC parameter set and key pair.</p> <p>FFC Schemes using "safe-prime" groups Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1.</p> <p><b>TD0580 has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: Safe Primes Key Generation CAVP #: A4573 Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

#### 7.3.4 FCS\_CKM.2 SP800-56A

Item	Data
<b>Test Assurance Activity</b>	<p>Key Establishment Schemes The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE using the applicable tests below.</p> <p>SP800-56A Key Establishment Schemes The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value <math>Z</math>) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag.</p> <p>Function Test</p>

	<p>The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested.</p> <p>The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information field OI and TOE id fields.</p> <p>If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret.</p> <p>The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values.</p> <p>If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm.</p> <p><b>Validity Test</b></p> <p>The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the other info and TOE id fields.</p> <p>The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).</p> <p>The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.</p>
<p><b>Pass/Fail with Explanation</b></p>	<p>Algorithm: KAS-ECC-SSC Sp800-56Ar3 and KAS-FFC-SSC Sp800-56Ar3</p> <p>CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>

<b>Result</b>	Pass
---------------	------

### 7.3.5 FCS\_CKM.2 RSA

Item	Data
<b>Test Assurance Activity</b>	RSA-based key establishment The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5.
<b>Pass/Fail with Explanation</b>	Algorithm: None. CCTL tested as per the PP/SD Evaluation Activities CAVP #: None. FTP_ITC.1 selects DTLS protocol that uses RSAES-PKCS1-v1_5. The test case FCS_DTSLC_EXT.1.1 Test #1 demonstrate the correctness of the TSF's implementation of RSAES-PKCS1-v1_5. This can be seen within the pcap files of the valid cipher tests indicating that the TOE supports TLS_RSA_WITH_AES_xxx ciphers, which uses a known good implementation of the RSAES-PKCS1-v1_5 key establishment scheme. Pass. Based on these findings, this assurance activity is considered satisfied.
<b>Result</b>	Pass

### 7.3.6 FCS\_CKM.2 FFC

Item	Data
<b>Test Assurance Activity</b>	FFC Schemes using "safe-prime" groups The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.
<b>Pass/Fail with Explanation</b>	Algorithm: KAS-FFC-SSC  CAVP #: A4573 Pass. Based on these findings, this assurance activity is considered satisfied.
<b>Result</b>	Pass

### 7.3.7 FCS\_COP.1/DataEncryption AES-CBC KAT

Item	Data
<b>Test Assurance Activity</b>	AES-CBC Known Answer Tests There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

	<p>KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key.</p> <p>To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.</p> <p>KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.</p> <p>To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.</p> <p>KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key <math>i</math> in each set shall have the leftmost <math>i</math> bits be ones and the rightmost <math>N-i</math> bits be zeros, for <math>i</math> in <math>[1,N]</math>.</p> <p>To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of keys and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key <math>i</math> in each set shall have the leftmost <math>i</math> bits be ones and the rightmost <math>N-i</math> bits be zeros, for <math>i</math> in <math>[1,N]</math>. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.</p> <p>KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value <math>i</math> in each set shall have the leftmost <math>i</math> bits be ones and the rightmost <math>128-i</math> bits be zeros, for <math>i</math> in <math>[1,128]</math>.</p> <p>To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: AES CBC  Key size: 128, 256  CAVP #: A4573  Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	<p>Pass</p>

### 7.3.8 FCS\_COP.1/DataEncryption AES-CBC MBMT

Item	Data
<b>Test Assurance Activity</b>	<p>AES-CBC Multi-Block Message Test</p> <p>The evaluator shall test the encrypt functionality by encrypting an i-block message where <math>1 &lt; i \leq 10</math>. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.</p> <p>The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where <math>1 &lt; i \leq 10</math>. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: AES CBC</p> <p>Key size: 128, 256</p> <p>CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

### 7.3.9 FCS\_COP.1/DataEncryption AES-CBC MCT

Item	Data
<b>Test Assurance Activity</b>	<p>AES-CBC Monte Carlo Tests</p> <p>The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:</p> <pre># Input: PT, IV, Key for i = 1 to 1000:   if i == 1:     CT[1] = AES-CBC-Encrypt(Key, IV, PT)     PT = IV   else:     CT[i] = AES-CBC-Encrypt(Key, PT)     PT = CT[i-1]</pre> <p>The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.</p> <p>The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AESCBC-Decrypt.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: AES CBC</p> <p>Key size: 128, 256</p> <p>CAVP #: A4573</p>

	Pass. Based on these findings, this assurance activity is considered satisfied.
<b>Result</b>	Pass

### 7.3.10 FCS\_COP.1/DataEncryption AES-GCM

Item	Data
<b>Test Assurance Activity</b>	<p>AES-GCM Test</p> <p>The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:</p> <p>128 bit and 256 bit keys</p> <p>a) Two plaintext lengths. One of the plaintext lengths shall be a nonzero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.</p> <p>a) Three AAD lengths. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.</p> <p>b) Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.</p> <p>The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.</p> <p>The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.</p> <p>The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: AES GCM</p> <p>Key size: 128, 256</p> <p>CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass



### 7.3.11 FCS\_COP.1/SigGen ECDSA

Item	Data
<b>Test Assurance Activity</b>	<p>ECDSA Algorithm Tests</p> <p>ECDSA FIPS 186-4 Signature Generation Test</p> <p>For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values R and S. To determine correctness, the evaluator shall use the signature verification function of a known good implementation.</p> <p>ECDSA FIPS 186-4 Signature Verification Test</p> <p>For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: ECDSA SigGen Curve: P-256 , P384 , P-521 CAVP #: A4573</p> <p>Algorithm: ECDSA SigVer Curve: P-256 , P384 , P-521 CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

### 7.3.12 FCS\_COP.1/SigGen RSA

Item	Data
<b>Test Assurance Activity</b>	<p>RSA Signature Algorithm Tests</p> <p>Signature Generation Test</p> <p>The evaluator generates or obtains 10 messages for each modulus size/SHA combination supported by the TOE. The TOE generates and returns the corresponding signatures.</p> <p>The evaluator shall verify the correctness of the TOE's signature using a trusted reference implementation of the signature verification algorithm and the associated public keys to verify the signatures.</p> <p>Signature Verification Test</p> <p>For each modulus size/hash algorithm selected, the evaluator generates a modulus and three associated key pairs, (d, e). Each private key d is used to sign six pseudorandom messages each of 1024 bits using a trusted reference implementation of the signature generation algorithm. Some of the public keys, e, messages, or signatures are altered so that signature verification should fail. For both the set of original messages and the set of altered messages: the modulus, hash algorithm, public key e values, messages, and signatures are forwarded to the TOE, which then attempts to verify the signatures and returns the verification results.</p>

	The evaluator verifies that the TOE confirms correct signatures on the original messages and detects the errors introduced in the altered messages.
<b>Pass/Fail with Explanation</b>	<p>Algorithm: RSA SigGen Key size / Modulus: 2048,3072,4096 CAVP #: A4573</p> <p>Algorithm: RSA SigVer Key size / Modulus: 2048,3072,4096 CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

### 7.3.13 FCS\_COP.1/Hash

Item	Data
<b>Test Assurance Activity</b>	<p>The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented testmacs.</p> <p>The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.</p> <p><b>Short Messages Test - Bit-oriented Mode</b> The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.</p> <p><b>Short Messages Test - Byte-oriented Mode</b> The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.</p> <p><b>Selected Long Messages Test - Bit-oriented Mode</b> The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the ith message is m + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.</p>

	<p>Selected Long Messages Test - Byte-oriented Mode</p> <p>The evaluators devise an input set consisting of <math>m/8</math> messages, where <math>m</math> is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the <math>i</math>th message is <math>m + 8 \cdot 99 \cdot i</math>, where <math>1 \leq i \leq m/8</math>. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.</p> <p>Pseudorandomly Generated Messages Test</p> <p>This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is <math>n</math> bits long, where <math>n</math> is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: SHA-1, SHA-256, SHA-384, SHA-512</p> <p>CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

#### 7.3.14 FCS\_COP.1/KeyedHash

Item	Data
<b>Test Assurance Activity</b>	For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key and message data using a known good implementation.
<b>Pass/Fail with Explanation</b>	<p>Algorithm: HMAC (SHA-1, SHA-256, SHA-384, SHA-512)</p> <p>CAVP #: A4573</p> <p>Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

#### 7.3.15 FCS\_RBG\_EXT.1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration.</p> <p>If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly</p>

	<p>generated. “generate one block of random bits” means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).</p> <p>If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.</p> <p>The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.</p> <p>Entropy input: the length of the entropy input value must equal the seed length.</p> <p>Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.</p> <p>Personalization string: The length of the personalization string must be &lt;= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.</p> <p>Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.</p>
<b>Pass/Fail with Explanation</b>	<p>Algorithm: CTR DRBG  Mode: AES 256  CAVP #: A4573  Pass. Based on these findings, this assurance activity is considered satisfied.</p>
<b>Result</b>	Pass

## 7.4 X509-Rev

Due to the nature of mutual authentication being required for DTLS connections, the testing performed in the FIA\_X509 module has been tested using different server/client commands. FIA\_X509\_EXT.1.1 Tests 3 & 4 and FIA\_X509\_EXT.3 Test 2 were tested with the TOE being the DTLS server while the remaining X509 tests were tested with the TOE behaving as a DTLS client. This was done to ensure that the behavior between server and client on the TOE were consistent and the TSF remained unchanged. The testing performed in the report reflects that the TOE treats both client and server certificates with the same requirements. All certificates are checked in the chain for revocation, expiration, modifications, etc. The evidence collected shows that there is no difference in behavior seen from the TOE whether it is acting as a server or client and therefore, the x509 functionality is the same regardless of where the TOE is in the connection.

### 7.4.1 FIA\_X509\_EXT.1.1/Rev Test #1a

Item	Data
<b>Test Assurance Activity</b>	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and

	shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator shows the connection attempt with packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should successfully allow all of the certificates to be processed.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful connection using the chain of certificates.
<b>Result</b>	Pass

#### 7.4.2 FIA\_X509\_EXT.1.1/Rev Test #1b

Item	Data
<b>Test Assurance Activity</b>	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator displays packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the connection as the chain of certificates is broken.
<b>Pass/Fail with Explanation</b>	Pass, The TOE doesn't allow the connection to start with the missing Intermediate certificate authority.
<b>Result</b>	Pass

#### 7.4.3 FIA\_X509\_EXT.1.1/Rev Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if

	<p>FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.</p>
<b>Test Steps</b>	<p>The ST states that “The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.” X.509v3 certificates are not used when performing trusted updates.</p> <ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator displays packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the connection attempt with an expired certificate.
<b>Pass/Fail with Explanation</b>	Pass, The TOE fails to successfully load the expired certificate.
<b>Result</b>	Pass

#### 7.4.4 FIA\_X509\_EXT.1.1/Rev Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 3: The evaluator shall test that the TOE can properly handle revoked certificates— conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.</p> <p>Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.</p>
<b>Test Steps</b>	<p>The ST states that “The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.” X.509v3 certificates are not used when performing trusted updates.</p> <p><u>OCSP</u></p>

	<p><b>Intermediate Valid</b></p> <ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator shows the connection attempt with packet capture evidence.</li> </ul> <p><b>Intermediate Revoked</b></p> <ul style="list-style-type: none"> <li>• The evaluator shows the chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE with a revoked ICA.</li> <li>• The evaluator shows the connection attempt with packet capture evidence.</li> </ul> <p><b>Leaf Valid</b></p> <ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator shows the connection attempt with packet capture evidence.</li> </ul> <p><b>Leaf Revoked</b></p> <ul style="list-style-type: none"> <li>• The evaluator shows the chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE with a revoked leaf certificate</li> <li>• The evaluator shows the connection attempt with packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject any DTLS server connection when either the intermediate certificate or the server certificate has been revoked.</li> <li>• The OCSP connection should show that the certificates have been revoked.</li> <li>• The Packet capture is expected to depict the specific certificate that is revoked, and the logs should verify that the TOE denies connection by denoting that the certificate has been revoked.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass The TOE successfully connects when using unrevoked certificates with a valid certificate chain, and denies connection when using revoked certificates, even if the certificate chain is valid.
<b>Result</b>	Pass

#### 7.4.5 FIA\_X509\_EXT.1.1/Rev Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.</p>

<b>Test Steps</b>	<p>The ST states that “The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.” X.509v3 certificates are not used when performing trusted updates.</p> <ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator attempts a connection to the TOE.</li> <li>• The evaluator shows the connection attempt with packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the connection with the missing OCSP signing purpose.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully rejects the connection as the OCSP responder is missing the OCSP signing purpose.
<b>Result</b>	Pass

#### 7.4.6 FIA\_X509\_EXT.1.1/Rev Test #5

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)</p>
<b>Test Steps</b>	<p>The ST states that “The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.” X.509v3 certificates are not used when performing trusted updates.</p> <ul style="list-style-type: none"> <li>• Upload a valid certificate chain on the TOE’s trustpoint.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the connection being successful.</li> <li>• Note the DTLS server certificate’s first eight bytes and the one byte that is to be modified.</li> <li>• Pass the previously noted fixed bytes, offset and new data bytes for the AcumenMITM tool to replace a byte in the first eight bytes in the DTLS server’s certificate.</li> <li>• Setup a server listening to allow DTLS connection on port 5001.</li> <li>• Initiate a DTLS connection from the TOE to the DTLS server.</li> <li>• Verify that the modification happens and the DTLS connection fails.</li> <li>• Verify the DTLS connection failure via TOE’s logs.</li> <li>• Verify the DTLS connection failure via packet capture.</li> </ul>



<b>Expected Test Results</b>	The TOE denies a DTLS connection when it is presented with a certificate that has been modified using the AcumenMITM tool. The tool modifies the first eight bytes of the certificate. The packet capture verifies that the DTLS connection is not established due to the bad certificate.
<b>Pass/Fail with Explanation</b>	Pass. The evaluator modified the first eight bytes of the certificate being presented by the server and ensured that the certificate fails to validate, and the TLS handshake fails. This meets the testing requirements.
<b>Result</b>	Pass

#### 7.4.7 FIA\_X509\_EXT.1.1/Rev Test #6

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)</p>
<b>Test Steps</b>	<p>The ST states that “The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.” X.509v3 certificates are not used when performing trusted updates.</p> <ul style="list-style-type: none"> <li>• Upload a valid certificate chain on the TOE’s trustpoint.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the connection being successful.</li> <li>• Note the bytes that are to be modified in signatureValue field of the DTLS server’s certificate.</li> <li>• Pass the previously noted fixed bytes, offset and new data bytes for the AcumenMITM tool to replace a byte in the signatureValue field in the DTLS server’s certificate.</li> <li>• Setup a server listening to allow DTLS connection on port 5001.</li> <li>• Initiate a DTLS connection from the TOE to the DTLS server.</li> <li>• Verify that the modification happens and the DTLS connection fails.</li> <li>• Verify the DTLS connection failure via TOE’s logs. Verify the DTLS connection failure via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE fails to establish a DTLS connection when the last bytes in the signatureValue field of the server’s certificate are modified using the AcumenMITM tool.</li> <li>• The packet capture proves that there is a decrypt error and the logs show that there is a failure in establishing DTLS connection. The packet capture proves that there is a decrypt error, and the logs show that there is a failure in establishing DTLS connection.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass The evaluator modified the first byte in the certificate signatureValue field and demonstrated that the certificate fails to validate. This meets the testing requirements.
<b>Result</b>	Pass

#### 7.4.8 FIA\_X509\_EXT.1.1/Rev Test #7

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)</p>
<b>Test Steps</b>	<p>The ST states that “The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for secure DTLS connections.” X.509v3 certificates are not used when performing trusted updates.</p> <ul style="list-style-type: none"> <li>• Upload a valid certificate chain on the TOE’s trustpoint.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the connection being successful.</li> <li>• Note the bytes that are to be modified in publickey of the DTLS server.</li> <li>• Pass the previously noted fixed bytes, offset and new data bytes for the AcumenMITM tool to replace bytes in the publickey field of DTLS server.</li> <li>• Setup a server listening to allow DTLS connection on port 5001.</li> <li>• Initiate a DTLS connection from the TOE to the DTLS server.</li> <li>• Verify that the modification happens and the DTLS connection fails.</li> <li>• Verify the DTLS connection failure via TOE’s logs.</li> <li>• Verify the DTLS connection failure via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE rejects a DTLS connection that is forged using the AcumenMITM tool to modify the DTLS server certificate such that its public key is modified.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects a DTLS connection when presented with a server having modified public key in its certificate.
<b>Result</b>	Pass

#### 7.4.9 FIA\_X509\_EXT.1.1/Rev Test #8a

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)</p> <p>(Conditional on support for a minimum certificate path length of three certificates)</p> <p>(Conditional on TOE ability to process CA certificates presented in certificate message)</p> <p>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.</p> <p><b>TD0527 (12/1 Update) has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<p>N/A. ST claims 'EC certificates are not supported for DTLS connections.'</p>

#### 7.4.10 FIA\_X509\_EXT.1.1/Rev Test #8b

Item	Data
<b>Test Assurance Activity</b>	<p>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)</p> <p>(Conditional on support for a minimum certificate path length of three certificates)</p> <p>(Conditional on TOE ability to process CA certificates presented in certificate message)</p> <p>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.</p> <p><b>TD0527 (12/1 Update) has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<p>N/A. ST claims 'EC certificates are not supported for DTLS connections.'</p>

#### 7.4.11 FIA\_X509\_EXT.1.1/Rev Test #8c

Item	Data
------	------

<b>Test Assurance Activity</b>	<p><b>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)</b></p> <p><b>(Conditional on support for a minimum certificate path length of three certificates)</b></p> <p>The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store.</p> <p><b>TD0527 (12/1 Update) has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<p>N/A. ST claims 'EC certificates are not supported for DTLS connections.'</p>

#### 7.4.12 FIA\_X509\_EXT.1.2/Rev Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.</p> <p>The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> <li>- a self-signed root CA certificate,</li> <li>- an intermediate CA certificate and</li> <li>- a leaf (node) certificate.</li> </ul> <p>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).</p> <p>Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:</p> <ul style="list-style-type: none"> <li>(i) <i>as part of the validation of the leaf certificate belonging to this chain;</i></li> <li>(ii) <i>(ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).</i></li> </ul>

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator shows the missing BasicConstraints Section of the certificate.</li> <li>• The evaluator demonstrates a connection attempt.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator displays packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject validation of the IntermediateCA as it is missing the BasicConstraints section.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow a certificate to be loaded with the missing BasicConstraints field.
<b>Result</b>	Pass

#### 7.4.13 FIA\_X509\_EXT.1.2/Rev Test #2

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.</p> <p>The goal of the following tests is to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> <li>• a self-signed root CA certificate,</li> <li>• an intermediate CA certificate and</li> <li>• a leaf (node) certificate.</li> </ul> <p>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).</p> <p>Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:</p> <ol style="list-style-type: none"> <li>1. As part of the validation of the leaf certificate belonging to this chain;</li> <li>2. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator shows the valid chain of certificates on the TOE.</li> <li>• The evaluator shows the BasicConstraints Section of the CA set to false.</li> </ul>

	<ul style="list-style-type: none"> <li>• The evaluator demonstrates a connection attempt.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator displays packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject validation of the IntermediateCA as the BasicConstraints Section is set to false.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow a certificate authority to be loaded with a false basic constraints field.
<b>Result</b>	Pass

#### 7.4.14 FIA\_X509\_EXT.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following test for each trusted channel:</p> <p>The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity.</p> <p>The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed.</p> <p>If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection where the certificate reaches out to a non-TOE IT entity.</li> <li>• The evaluator demonstrates evidence that the certificate was invalidated, and the connection fails.</li> </ul>
<b>Expected Test Results</b>	The TOE does not allow a certificate to be validated that contains invalid credentials.
<b>Pass/Fail with Explanation</b>	Pass, The TOE attempts to reach out to the non-TOE entity and fails as the entity is not present.
<b>Result</b>	Pass

#### 7.4.15 FIA\_X509\_EXT.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the

	format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator generates a certificate request.</li> <li>• The evaluator shows evidence of the formatting of the generated certificate request.</li> </ul>
<b>Expected Test Results</b>	The TOE should successfully allow a certificate request to be generated.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully generates a certificate signing request with the required information.
<b>Result</b>	Pass

#### 7.4.16 FIA\_X509\_EXT.3 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator generates a certificate signing request on the TOE.</li> <li>• The evaluator makes a connection attempt when the certificate authority is not loaded into the trust store, and the logs verify that it fails.</li> <li>• The evaluator uploads the CA to the TOE.</li> <li>• The evaluator displays the certificate authority to the TOE.</li> <li>• The evaluator makes a connection attempt.</li> <li>• The evaluator displays packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow successful validation due to an incomplete cert path. The evaluator will then demonstrate successful validation with a root and intermediate CA.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful connection from a correctly formed certificate chain and rejects connection when the certificate chain is incomplete.
<b>Result</b>	Pass

## 7.5 DTLSS

### 7.5.1 FCS\_DTLSS\_EXT.1.1 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	Test 1: The evaluator shall establish a DTLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA The evaluator verifies the connection with logs from the TOE. The evaluator verifies the connection with a packet capture.</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA The evaluator verifies the connection with logs from the TOE. The evaluator verifies the connection with a packet capture.</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA256 The evaluator verifies the connection with logs from the TOE. The evaluator verifies the connection with a packet capture.</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA256 The evaluator verifies the connection with logs from the TOE. The evaluator verifies the connection with a packet capture.</li> <li>• TLS_RSA_WITH_AES_128_GCM_SHA256 The evaluator verifies the connection with logs from the TOE. The evaluator verifies the connection with a packet capture.</li> <li>• TLS_RSA_WITH_AES_256_GCM_SHA384 The evaluator verifies the connection with logs from the TOE. The evaluator verifies the connection with a packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should be able to make each connection using the supported ciphersuite.
<b>Pass/Fail with Explanation</b>	Pass, The test passes as the TOE uses all of the required cipher suites that are in the requirements of the security target documentation.
<b>Result</b>	Pass

### 7.5.2 FCS\_DTLSS\_EXT.1.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection.



	Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
<b>Test Steps</b>	<p>Part 1</p> <ul style="list-style-type: none"> <li>• The evaluator uses the Acumen MITM tool to send a cipher suite that isn't supported in the ST.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of packet capture.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of logs.</li> </ul> <p>Part 2</p> <ul style="list-style-type: none"> <li>• The evaluator uses the Acumen MITM tool to send a NULL_with_NULL_NULL cipher suite.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of packet capture.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the different unsupported cipher suites.
<b>Pass/Fail with Explanation</b>	<p>Part 1</p> <ul style="list-style-type: none"> <li>• The test passes since there is a connection failure upon inserting an incorrect cipher suite on the handshake.</li> </ul> <p>Part 2</p> <ul style="list-style-type: none"> <li>• The test passes upon inserting the TLS_NULL_WITH_NULL_NULL into the handshake causes the connection to timeout.</li> </ul>
<b>Result</b>	Pass

### 7.5.3 FCS\_DTLSS\_EXT.1.1 Test #3a

Item	Data
<b>Test Assurance Activity</b>	Modify a byte in the Client Finished handshake message and verify that the server rejects the connection and does not send any application data.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator uses the Acumen MITM tool to modify a byte in the Client Finished message.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of packet capture.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should discard the connection after a byte in the Client Finished message is modified.
<b>Pass/Fail with Explanation</b>	Pass, The TOE discards the connection attempt after a byte in the client finished message is modified.
<b>Result</b>	Pass

### 7.5.4 FCS\_DTLSS\_EXT.1.1 Test #3b

Item	Data
<b>Test Assurance Activity</b>	<p>(Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.)</p> <p>The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent.</p> <p>The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message.</p> <p>The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt a TLS connection with the TOE using claimed cipher suites and ensure the connection being accepted.</li> <li>• Verify that no Alert with alert level Fatal (2) messages were sent.</li> <li>• Verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message.</li> <li>• Examine the Finished message and confirm that it does not contain unencrypted data by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE should reject a connection when text is not encrypted otherwise it should succeed.</li> <li>• Evidence (Packet capture) showing the message is encrypted hence the connection is successful.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. The Finished message contains Hexadecimal 16 and is sent immediately after Hexadecimal 14 in the ChangeCipherSpec message. The first byte of the encrypted Finished message does not equal hexadecimal 14. This meets the testing requirement.
<b>Result</b>	Pass

### 7.5.5 FCS\_DTLSS\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	Modify at least one byte in the cookie from the Server's HelloVerifyRequest message and verify that the Server rejects the Client's handshake message.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator uses the Acumen MITM tool to modify a byte in the cookie of the HelloVerifyRequest of the server.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of packet capture.</li> <li>• The evaluator verifies the unsuccessful DTLS connection with the help of logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow a successful connection with a modified byte in the cookie of the HelloVerifyRequest
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not successfully connect after a byte in the cookie is modified.
<b>Result</b>	Pass

### 7.5.6 FCS\_DTLSS\_EXT.1.4 Test #1a

Item	Data
<b>Test Assurance Activity</b>	<p>If <b>ECDHE ciphersuites</b> are supported:</p> <p>The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The evaluator shall verify (through a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.</p>
<b>Pass/Fail with Explanation</b>	N/A. The ST does not select ECDHE ciphersuites.

### 7.5.7 FCS\_DTLSS\_EXT.1.4 Test #1b

Item	Data
<b>Test Assurance Activity</b>	If <b>ECDHE ciphersuites</b> are supported:

	The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.
<b>Pass/Fail with Explanation</b>	N/A. The ST does not select ECDHE ciphersuites.

### 7.5.8 FCS\_DTLSS\_EXT.1.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>If <b>DHE ciphersuites</b> are supported, the evaluator shall repeat the following test for each supported parameter size.</p> <p>If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the configured Diffie-Hellman parameter size(s).</p>
<b>Pass/Fail with Explanation</b>	N/A. The ST does not select DHE ciphersuites.

### 7.5.9 FCS\_DTLSS\_EXT.1.4 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>If <b>RSA key establishment ciphersuites</b> are supported, the evaluator shall repeat this test for each RSA key establishment key size.</p> <p>If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.</p>
<b>Test Steps</b>	<p>RSA-2048</p> <ul style="list-style-type: none"> <li>• The evaluator attempts a connection.</li> <li>• The evaluator verifies the connection with logs from the TOE.</li> <li>• The evaluator verifies the connection with a packet capture.</li> </ul> <p>RSA-3072</p> <ul style="list-style-type: none"> <li>• The evaluator attempts a connection.</li> <li>• The evaluator verifies the connection with logs from the TOE.</li> </ul>

	<ul style="list-style-type: none"> <li>The evaluator verifies the connection with a packet capture.</li> </ul> <p>RSA-4096</p> <ul style="list-style-type: none"> <li>The evaluator attempts a connection.</li> <li>The evaluator verifies the connection with logs from the TOE.</li> <li>The evaluator verifies the connection with a packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should successfully connect using all of the supported key establishment sizes
<b>Pass/Fail with Explanation</b>	Pass The test passes as all 3 different supported key sizes were generated and loaded in the TOE.
<b>Result</b>	Pass

### 7.5.10 FCS\_DTLSS\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall establish a connection using a client. The evaluator will then modify at least one byte in a record message and verify that the Server discards the record or terminates the DTLS session.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Upload a valid certificate chain on the TOE.</li> <li>Configure the TOE as a DTLS server to accept connections on port 5001.</li> <li>Initiate a connection from the DTLS client to the TOE and show the connection being successful.</li> <li>Note the record message data of the DTLS client that is to be modified.</li> <li>Pass the previously noted fixed bytes, offset and new data bytes for the AcumenMITM tool to replace the bytes in the record data of the DTLS client's certificate.</li> <li>Verify that the modification happens and the DTLS connection fails.</li> <li>Verify the DTLS connection failure via TOE's logs.</li> <li>Verify the DTLS connection failure via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE terminates and discards the connection due to a modification in the record message of the DTLS client.
<b>Pass/Fail with Explanation</b>	Pass. The TOE terminates the DTLS connection with the client having modified record data in its certificate.
<b>Result</b>	Pass

### 7.5.11 FCS\_DTLSS\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall set up a DTLS connection. The evaluator shall then capture traffic sent from the DTLS Client to the TOE. The evaluator shall retransmit copies of this traffic to the TOE in order to impersonate the DTLS Client. The evaluator shall observe that the TSF does not take action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Upload a valid certificate on the TOE.</li> <li>• Configure the TOE to act as a server.</li> <li>• Establish a successful connection with the TOE from the DTLS client (VM).</li> <li>• Verify the successful connection via packet capture.</li> <li>• Verify the logs for the successful connection.</li> <li>• Segregate just the traffic captured from the DTLS client.</li> <li>• Retransmit the previous captured traffic of the successful DTLS connection to the TOE in order to impersonate the DTLS client.</li> <li>• Verify the unsuccessful DTLS connection via TOE's log.</li> <li>• Verify that the TOE does not respond to the impersonated DTLS client via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should not take any action in response to receiving replay traffic form the impersonated DTLS client and the TOE'S audit log should indicate that the replayed traffic was discarded.
<b>Pass/Fail with Explanation</b>	Pass. The evaluator has verified TOE does not take action in response to retransmitted traffic and that the audit log indicates that the replayed traffic was discarded.
<b>Result</b>	Pass

### 7.5.12 FCS\_DTLSS\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>If the <b>TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077</b>, the evaluator shall perform the following test:</p> <ol style="list-style-type: none"> <li>a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket.</li> <li>b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake).</li> <li>c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps:</li> </ol> <p>Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID.</p>

	<p>d) The client completes the TLS handshake and captures the SessionID from the ServerHello.</p> <p>e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session from step d) open or by starting a new TLS session using the SessionID captured in step d).</p> <p>f) The client verifies the TOE (1) implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt a TLS connection with a zero-length session identifier and a zero-length session ticket.</li> <li>• Verify with packet capture that the client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length session ticket.</li> <li>• Verify with packet capture that the server does not send a NewSessionTicket handshake message (at any point in the handshake).</li> <li>• Verify that the Server Hello message contains a non-zero session identifier.</li> <li>• Verify with packet capture that client sends a ClientHello containing the SessionID captured on the previous Server Hello SessionID.</li> <li>• Verify with packet capture that the handshake is successful with a different SessionID sent on the ServerHello.</li> </ul>
<b>Expected Test Results</b>	The TOE should successfully display separate SessionID's.
<b>Pass/Fail with Explanation</b>	Pass. TOE does not support session resumption based on session IDs or session ticket. This meets the testing requirements.
<b>Result</b>	Pass

### 7.5.13 FCS\_DTLSS\_EXT.1.7 Test 2a

Item	Data
<b>Test Assurance Activity</b>	<p>If the TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2), the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <p>The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages (as shown in figure 2 of RFC 4346 or RFC 5246).</p>
<b>Pass/Fail with Explanation</b>	N/A. The ST does not support selection for session resumption using session IDs.

#### 7.5.14 FCS\_DTLSS\_EXT.1.7 Test 2b

Item	Data
Test Assurance Activity	<p>If the <b>TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)</b>, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <p>The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its ChangeCipherSpec message thereby disrupting the handshake. The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.</p>
Pass/Fail with Explanation	N/A. The ST does not support selection for session resumption using session IDs.

#### 7.5.15 FCS\_DTLSS\_EXT.1.7 Test 3a

Item	Data
Test Assurance Activity	<p>If the <b>TOE supports session tickets according to RFC5077</b>, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <p>The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with a ServerHello with an empty SessionTicket extension, NewSessionTicket, ChangeCipherSpec and Finished messages (as seen in figure 2 of RFC 5077).</p>
Pass/Fail with Explanation	N/A. The TOE does not support selection for session tickets.

#### 7.5.16 FCS\_DTLSS\_EXT.1.7 Test 3b

Item	Data
Test Assurance Activity	<p>If the <b>TOE supports session tickets according to RFC5077</b>, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <p>The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator will then modify the session ticket and send it as</p>



	part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.
<b>Pass/Fail with Explanation</b>	N/A. The TOE does not support selection for session tickets.

## 7.6 DTLSS-MA

### 7.6.1 FCS\_DTLSS\_EXT.2.1&2.2 Test #1a

Item	Data
<b>Test Assurance Activity</b>	Test 1a [conditional]: If the TOE requires or can be configured to require a client certificate, the evaluator shall configure the TOE to require a client certificate and send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate_list structure with a length of zero in the Client Certificate message. The evaluator shall verify that the handshake is not finished successfully and no application data flows.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure Acumen-MITM tool to modify a length of zero in the Client Certificate message client's Certificate.</li> <li>• Verify that the Acumen MITM tool found specified byte match to modify it.</li> <li>• Attempt a TLS connection from the VM to TOE.</li> <li>• Verify the connection was not successful using packet capture.</li> <li>• Verify the connection was not successful using log.</li> </ul>
<b>Expected Test Results</b>	The TOE rejects the TLS connection when the client does not provide its certificate.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects the connection when the client tries to connect with the zero Length certificate. This meets the testing requirements
<b>Result</b>	Pass

### 7.6.2 FCS\_DTLSS\_EXT.2.1&2.2 Test #1b

Item	Data
<b>Test Assurance Activity</b>	Test 1b [conditional]: If the TOE supports fallback authentication functions and these functions cannot be disabled, the evaluator shall configure the fallback authentication functions on the TOE and configure the TOE to send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate_list structure with a length of zero in the Client Certificate message. The evaluator shall verify the TOE authenticates the connection using the fallback authentication functions as described in the TSS. Note: Testing the validity of the client certificate is performed as part of X.509 testing.
<b>Pass/Fail with Explanation</b>	NA, the fallback authentication function is not implemented. Hence this Test case is not applicable.

### 7.6.3 FCS\_DTLSS\_EXT.2.1&2.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2 [conditional]: If DTLS 1.2 is claimed for the TOE, the evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the MITM tool such that it changes Server Certificate request with unsupported signature algorithm (MD5_RSA) .</li> <li>• Initiate a connection from the DTLS client to the TOE (Server) and show the unsuccessful connection.</li> <li>• Initiate a connection from the TOE to the DTLS Client and show the unsuccessful connection.</li> <li>• Verify that the connection is not established through packet capture Verify that a log is generated indicating that connection was terminated.</li> </ul>
<b>Expected Test Results</b>	The TOE denies a TLS connection initiated using a client certificate without the supported_signature_algorithm
<b>Pass/Fail with Explanation</b>	Pass. TOE rejects mutually authenticated TLS connection attempts from a client whose certificate contains an unsupported signature algorithm.
<b>Result</b>	Pass

### 7.6.4 FCS\_DTLSS\_EXT.2.1&2.2 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3: The aim of this test is to check the response of the server when it receives a client identity certificate that is signed by an impostor CA (either Root CA or intermediate CA). To carry out this test the evaluator shall configure the client to send a client identity certificate with an issuer field that identifies a CA recognised by the TOE as a trusted CA, but where the key used for the signature on the client certificate does not correspond to the CA certificate trusted by the TOE (meaning that the client certificate is invalid because its certification path does not terminate in the claimed CA certificate). The evaluator shall verify that the attempted connection is denied.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the TOE CA details.</li> <li>• Create a CA certificate whose CN matches with the CA certificate on the TOE but with a different key. Then sign the client certificate with this CA with the different key. CN matches with the CA certificate on the TOE</li> <li>• Attempt to connect to the TOE with the new client certificate and show the connection fails.</li> <li>• Verify the failure logs on the device.</li> <li>• Verify the failure with packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE rejects a TLS connection initiated using an impostor CA.</li> <li>• Logs show the connection failure.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. TOE rejects mutually authenticated TLS connection attempts from a client whose certificate is invalid since the signature does not correspond to the trusted CA.
<b>Result</b>	Pass

#### 7.6.5 FCS\_DTLSS\_EXT.2.1&2.2 Test #4

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the client to send a certificate with the Client Authentication purpose in the extendedKeyUsage field and verify that the server accepts the attempted connection. The evaluator shall repeat this test without the Client Authentication purpose and shall verify that the server denies the connection. Ideally, the two certificates should be identical except for the Client Authentication purpose.
<b>Test Steps</b>	<p>Part 1</p> <ul style="list-style-type: none"> <li>Attempt to establish the connection using a TLS server with a client certificate that contains the Client Authentication purpose in the extendedKeyUsage field.</li> <li>Attempt a TLS connection from the TOE to the TLS Client.</li> <li>Verify the connection was successful via log.</li> <li>Verify the connection was successful via packet capture.</li> </ul> <p>Part 2</p> <ul style="list-style-type: none"> <li>Attempt to establish the connection using a TLS Client with a Client certificate that lacks the Client Authentication purpose in the extendedKeyUsage field.</li> <li>Attempt a TLS connection from the TOE to the TLS Client.</li> <li>Verify the connection was not successful via log.</li> <li>Verify the connection was not successful via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>TOE accepts a TLS connection initiated using a client certificate containing the Client Authentication purpose.</li> <li>TOE denies a TLS connection initiated using a client certificate missing the Client Authentication purpose.</li> <li>TOE logs show the failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE accepts the connections from client with certificates containing the client Authentication purpose in the extendedKeyUsage extension and rejecting connections from client whose certificates lack client Authentication purpose in the extendedKeyUsage extension. This meets the testing requirement.
<b>Result</b>	Pass

#### 7.6.6 FCS\_DTLSS\_EXT.2.1&2.2 Test #5a

Item	Data
<b>Test Assurance Activity</b>	<p>Test 5: The evaluator shall perform the following modifications to the traffic:</p> <p>a) Configure the server to require mutual authentication and then connect to the server with a client configured to send a client certificate that is signed by a Certificate Authority trusted by the TOE. The evaluator shall verify that the server accepts the connection.</p>

<b>Pass/Fail with Explanation</b>	Refer to testcase FCS_DTLSS_EXT.2.1&2.2 Test #6.
<b>Result</b>	Pass

### 7.6.7 FCS\_DTLSS\_EXT.2.1&2.2 Test #5b

Item	Data
<b>Test Assurance Activity</b>	Test 5: The evaluator shall perform the following modifications to the traffic: b) Configure the server to require mutual authentication and then modify a byte in the signature block of the client's Certificate Verify handshake message (see RFC5246 Sec 7.4.8). The evaluator shall verify that the server rejects the connection.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure Acumen-MITM tool to modify a byte in the signature block of the client's Certificate.</li> <li>• Verify that the Acumen MITM tool found specified byte match to modify it</li> <li>• Attempt a TLS connection from the VM to TOE</li> <li>• Verify the connection was not successful using packet capture.</li> <li>• Verify the connection was not successful using log.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE rejects a TLS connection when presented with a client certificate with a modified byte in the signature block.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The evaluator verified the server rejects the connection when a byte is modified in the signature block of the client's Certificate Verify handshake message. This meets the testing requirements.
<b>Result</b>	Pass

### 7.6.8 FCS\_DTLSS\_EXT.2.1&2.2 Test #6

Item	Data
<b>Test Assurance Activity</b>	<p>Note: Testing the validity of the client certificate is performed as part of X.509 testing.</p> <p>The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows:</p> <p>Test 6: Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.</p>
<b>Test Steps &amp; Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Upload a complete certificate validation chain to the TOE.</li> <li>• Initiate a connection with the TOE over TLS and show the connection being successful.</li> <li>• Verify the successful connection via packet capture.</li> <li>• Verify the successful connection via TOE Logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to successfully establish a DTLS connection when a complete chain of certificates is presented.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. When complete CA certificates are present, the TOE is able to make a trusted channel/connection. This meets the testing requirements.
<b>Result</b>	Pass

### 7.6.9 FCS\_DTLSS\_EXT.2.1&2.2 Test #7

Item	Data
<b>Test Assurance Activity</b>	Test 7: The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
<b>Test Steps</b>	<ol style="list-style-type: none"> <li>1. Failed matching of the reference identifier <ul style="list-style-type: none"> <li>• Create a client certificate containing an unexpected reference identifier.</li> <li>• Initiate a TLS connection to the TOE with the above client certificate and verify that it fails.</li> <li>• Verify failure logs.</li> <li>• Verify connection failure via packet capture.</li> </ul> </li> <li>2. Failed validation of the certificate path <ul style="list-style-type: none"> <li>• Verify the CA certificate chain located on the TOE.</li> <li>• Remove the ICA from the CA certificate chain.</li> <li>• Verify that the TOE breaks the connection leading to connection failure.</li> <li>• Verify the connection failure logs on the TOE.</li> <li>• Verify connection failure via packet capture.</li> </ul> </li> <li>3. Failed validation of the expiration date <ul style="list-style-type: none"> <li>• Create an expired Server certificate.</li> <li>• Replace the Server certificate( Device-cert) with the expired certificate.</li> <li>• Verify the failure logs on the TOE.</li> </ul> </li> <li>4. Failed determination of the revocation status <ul style="list-style-type: none"> <li>• Verify the valid chain of OCSP certificates on the TOE.</li> <li>• Create an client certificate with missing OCSP signing flag.</li> <li>• Initiate a TLS connection to the TOE with the above created certificate.</li> <li>• Verify connection failure via packet capture.</li> </ul> </li> </ol>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE denies a connection initiated using a client certificate containing an unexpected reference identifier.</li> <li>• The TOE rejects the connection when an incomplete certificate trust chain is present.</li> <li>• The TOE should deny connection when the certificate is expired.</li> <li>• The TOE doesn't establish a connection when the OCSP signing purpose is missing and validation fails.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. TOE rejects the connection from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, and failed determination of the revocation status.
<b>Result</b>	Pass

### 7.6.10 FCS\_DTLSS\_EXT.2.1&2.2 Test #8

Item	Data
<b>Test Assurance Activity</b>	Test 8 [conditional]: The purpose of this test is to verify that only selected certificate validation failures could be administratively overridden. If any override mechanism is defined for failed certificate validation, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
<b>Pass/Fail with Explanation</b>	NA, TOE does not implement any administrator override mechanism.

### 7.6.11 FCS\_DTLSS\_EXT.2.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall send a client certificate with an identifier that does not match an expected identifier and verify that the server denies the connection.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a certificate with a mismatched (CN) identifier.</li> <li>• Attempt to connect to the TOE with this certificate.</li> <li>• Verify with logs that the connection is denied because the identifier (CN) is not recognized.</li> <li>• Verify with packet capture that the connection is denied because the identifier (CN) is not recognized.</li> </ul>
<b>Expected Test Results</b>	TOE denies a TLS connection initiated using a client certificate containing an unexpected reference identifier.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects connection when a client certificate has an identifier that does not match an expected identifier.
<b>Result</b>	Pass

## 7.7 DTLSC

### 7.7.1 FCS\_DTLSC\_EXT.1.1 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall establish a DTLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).</p>
<b>Test Steps</b>	<p><b>TLS_RSA_WITH_AES_128_CBC_SHA</b></p> <ul style="list-style-type: none"> <li>• Configure a server using openssl to listen for incoming connections and restrict the supported cipher suite to only AES_128_CBC_SHA.</li> <li>• Initiate the SDWAN interface on the TOE and verify the successful connection with the server.</li> <li>• Verify via packet capture that the selected cipher suite was used.</li> </ul> <p><b>TLS_RSA_WITH_AES_256_CBC_SHA</b></p> <ul style="list-style-type: none"> <li>• Configure a server using openssl to listen for incoming connections and restrict the supported cipher suite to only AES_256_CBC_SHA.</li> <li>• Initiate the SDWAN interface on the TOE and verify the successful connection with the server.</li> <li>• Verify via packet capture that the selected cipher suite was used.</li> </ul> <p><b>TLS_RSA_WITH_AES_128_CBC_SHA256</b></p> <ul style="list-style-type: none"> <li>• Configure a server using openssl to listen for incoming connections and restrict the supported cipher suite to only AES_128_CBC_SHA256.</li> <li>• Initiate the SDWAN interface on the TOE and verify the successful connection with the server.</li> <li>• Verify via packet capture that the selected cipher suite was used.</li> </ul> <p><b>TLS_RSA_WITH_AES_256_CBC_SHA256</b></p> <ul style="list-style-type: none"> <li>• Configure a server using openssl to listen for incoming connections and restrict the supported cipher suite to only AES_256_CBC_SHA256.</li> <li>• Initiate the SDWAN interface on the TOE and verify the successful connection with the server.</li> <li>• Verify via packet capture that the selected cipher suite was used.</li> </ul> <p><b>TLS_RSA_WITH_AES_128_GCM_SHA256</b></p> <ul style="list-style-type: none"> <li>• Configure a server using openssl to listen for incoming connections and restrict the supported cipher suite to only AES_128_GCM_SHA256.</li> <li>• Initiate the SDWAN interface on the TOE and verify the successful connection with the server.</li> <li>• Verify via packet capture that the selected cipher suite was used.</li> </ul> <p><b>TLS_RSA_WITH_AES_256_GCM_SHA384</b></p> <ul style="list-style-type: none"> <li>• Configure a server using openssl to listen for incoming connections and restrict the supported cipher suite to only AES_256_GCM_SHA384.</li> </ul>

	<ul style="list-style-type: none"> <li>• Initiate the SDWAN interface on the TOE and verify the successful connection with the server.</li> <li>• Verify via packet capture that the selected cipher suite was used.</li> </ul>
<b>Expected Test Results</b>	The TOE must be able to establish a successful DTLS connection with the DTLS server using the claimed ciphersuites.
<b>Pass/Fail with Explanation</b>	Pass. TOE successfully negotiates each of the claimed cipher suites. This meets the test requirements
<b>Result</b>	Pass

### 7.7.2 FCS\_DTLSC\_EXT.1.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The goal of the following test is to verify that the TOE accepts only certificates with appropriate values in the extendedKeyUsage extension, and implicitly that the TOE correctly parses the extendedKeyUsage extension as part of X.509v3 server certificate validation.</p> <p>Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.</p>
<b>Test Steps &amp;</b>	<p><u>Part 1</u></p> <ul style="list-style-type: none"> <li>• Create a server certificate with the Server Authentication EKU.</li> <li>• Attempt a connection from the TOE to a DTLS server on port 5001 that contains certificate with the Server Authentication EKU and verify the connection succeeds.</li> <li>• Verify the connection was successful via TOE's logs.</li> <li>• Verify the connection was successful via packet capture.</li> </ul> <p><u>Part 2</u></p> <ul style="list-style-type: none"> <li>• Create a server certificate without the Server Authentication EKU.</li> <li>• Attempt a connection from the TOE to a DTLS server on port 5001 that contains certificate with missing Server Authentication EKU and verify the connection fails.</li> <li>• Verify the connection was not successful via TOE's logs.</li> <li>• Verify the connection was not successful via packet capture.</li> </ul>
<b>Expected Test Results</b>	TOE should establish a connection with a server with authorized server certificate otherwise TOE should reject the connection.



<b>Pass/Fail with Explanation</b>	Pass. The TOE accepts the connections from server with certificates containing the Server Authentication purpose in the extendedKeyUsage extension and rejecting connections from server whose certificates lack Server Authentication purpose in the extendedKeyUsage extension. This meets the testing requirement.
<b>Result</b>	Pass

### 7.7.3 FCS\_DTLSC\_EXT.1.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3: The evaluator shall send a server certificate in the DTLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the DTLS_RSA_WITH_AES_128_CBC_SHA ciphersuite). The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the MITM tool such that it changes the RSA Cipher to ECDSA (non-Supported) in the server certificate.</li> <li>• Initiate a connection from the DTLS server to the TOE with RSA Certificates and show the unsuccessful connection.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the unsuccessful connection.</li> <li>• Verify that the connection is not established through packet capture.</li> <li>• Verify that a log is generated indicating that the connection was terminated.</li> </ul>
<b>Expected Test Results</b>	The TOE should be unable to establish a connection with a non-supported ciphersuite.
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied the connection to a server using an Unsupported ciphersuite. This meets the testing requirements.
<b>Result</b>	Pass

### 7.7.4 FCS\_DTLSC\_EXT.1.1 Test #4a

Item	Data
<b>Test Assurance Activity</b>	Test 4: The evaluator shall perform the following 'negative tests': <ul style="list-style-type: none"> <li>a) The evaluator shall configure the server to select the DTLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.</li> </ul>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the MITM tool such that it changes the RSA Cipher to TLS_NULL_WITH_NULL_NULL in the server certificate.</li> <li>• Initiate a connection from the DTLS server to the TOE with RSA Certificates and show the unsuccessful connection.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the unsuccessful connection.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify that the connection is not established through packet capture.</li> <li>• Verify that a log is generated indicating that connection was terminated.</li> </ul>
<b>Expected Test Results</b>	The TOE denies any connection to a server with TLS_NULL_WITH_NULL_NULL.
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied the connection to a server using a NULL ciphersuite. This meets the testing requirement.
<b>Result</b>	Pass

#### 7.7.5 FCS\_DTLSC\_EXT.1.1 Test #4b

Item	Data
<b>Test Assurance Activity</b>	Test 4: The evaluator shall perform the following 'negative tests': <ul style="list-style-type: none"> <li>b) Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test requirements are covered by FCS_DTLSC_EXT.1.1 Test #3.
<b>Result</b>	Pass

#### 7.7.6 FCS\_DTLSC\_EXT.1.1 Test #4c

Item	Data
<b>Test Assurance Activity</b>	Test 4: The evaluator shall perform the following 'negative tests': <ul style="list-style-type: none"> <li>c) [conditional]: If the TOE presents the <b>Supported Elliptic Curves/Supported Groups Extension</b> the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the DTLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.</li> </ul>
<b>Pass/Fail with Explanation</b>	NA, TOE Does not support Elliptic Curves/Groups Extension.

#### 7.7.7 FCS\_DTLSC\_EXT.1.1 Test #5a

Item	Data
<b>Test Assurance Activity</b>	Test 5: The evaluator performs the following modifications to the traffic:

	a) Change the DTLS version selected by the server in the Server Hello to a non-supported DTLS version and verify that the client rejects the connection.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the MITM tool such that it changes DTLS Version to DTLS 1.0 in the server Hello.</li> <li>• Initiate a connection from the DTLS server to the TOE with Certificates and show the unsuccessful connection.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the unsuccessful connection.</li> <li>• Verify that the connection is not established through packet capture.</li> <li>• Verify that a log is a generated indicating that connection was terminated.</li> </ul>
<b>Expected Test Results</b>	The TOE denies any connection where the DTLS version in the server is a non-supported DTLS version.
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied the connection to a server using a unsupported Protocol version. This meets the testing requirement.
<b>Result</b>	Pass

### 7.7.8 FCS\_DTLSC\_EXT.1.1 Test #5b

Item	Data
<b>Test Assurance Activity</b>	<p>Test 5: The evaluator performs the following modifications to the traffic:</p> <p>b) [conditional]: If <b>using DHE or ECDH</b>, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with DTLS, then this test shall be omitted.</p>
<b>Pass/Fail with Explanation</b>	NA, TOE does not support DHE or ECDH.

### 7.7.9 FCS\_DTLSC\_EXT.1.1 Test #6a

Item	Data
<b>Test Assurance Activity</b>	<p>Test 6: The evaluator performs the following 'scrambled message tests':</p> <p>a) Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the MITM tool such that it modifies a byte in the Server Finished handshake.</li> <li>• Initiate a connection from the DTLS server to the TOE and show the connection</li> <li>• Initiate a connection from the TOE to the DTLS server.</li> <li>• Verify the connection and verify through packet capture. that handshake does not finish successfully, and no application data flows</li> <li>• Verify that a log is a generated indicating that connection was terminated.</li> </ul>

<b>Expected Test Results</b>	The TOE denies a connection to a server when a byte is modified in the server finished handshake message
<b>Pass/Fail with Explanation</b>	Pass. The evaluator verified that the handshake does not finish successfully, and no application data flows when a byte is modified in the Server Finished handshake message. This meets the testing requirements.
<b>Result</b>	Pass

#### 7.7.10 FCS\_DTLS\_EXT.1.1 Test #6b

Item	Data
<b>Test Assurance Activity</b>	Test 6: The evaluator performs the following 'scrambled message tests':  b) Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the MITM tool to send a garbled message from the server after the server has issued the ChangeCipherSpec message.</li> <li>• Initiate a connection from the DTLS server to the TOE and show the unsuccessful connection.</li> <li>• Initiate a connection from the TOE to the DTLS server.</li> <li>• Verify that the connection and verify through packet capture that handshake does not finish successfully and no application data flows</li> <li>• Verify that a log is a generated indicating that connection was terminated.</li> </ul>
<b>Expected Test Results</b>	The TOE denies a connection when a garbled message is received from the server after the server has issues the ChangeCipherSpec message
<b>Pass/Fail with Explanation</b>	Pass. The evaluator verified that the handshake does not finish successfully, and no application data flows when a garbled message is sent from the server after the server has issued the ChangeCipherSpec message. This meets the testing requirements.
<b>Result</b>	Pass

#### 7.7.11 FCS\_DTLS\_EXT.1.1 Test #6c

Item	Data
<b>Test Assurance Activity</b>	Test 6: The evaluator performs the following 'scrambled message tests':  c) Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.

<b>Pass/Fail with Explanation</b>	NA, TOE does not support DHE or ECDH
-----------------------------------	--------------------------------------

### 7.7.12 FCS\_DTLSC\_EXT.1.2 Test #1

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 1 [conditional]: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN.</p> <p>Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <ul style="list-style-type: none"> <li><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></li> <li><i>Or:</i></li> <li><i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></li> </ul> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li><i>• IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Test Steps</b>	<p><b><u>Part 1 - IPv4</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv4.</li> </ul>

	<ul style="list-style-type: none"> <li>• Create a certificate with incorrect CN and missing SAN.</li> <li>• Start the TLS server with certificate which has incorrect CN and missing SAN.</li> <li>• Attempt the connection from TOE to the TLS server.</li> <li>• Verified with log that connection was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul> <p><b>Part 2 – IPv6</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv6.</li> <li>• Create a Server certificate with incorrect CN and missing SAN.</li> <li>• Start the TLS server with certificate which has incorrect CN and missing SAN.</li> <li>• Attempt the connection from TOE to the TLS server.</li> <li>• Verified with log that connection was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul> <p><b>Part 3 - FQDN</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as FQDN.</li> <li>• Configure the Server certificate showing incorrect CN and missing SAN.</li> <li>• Start the TLS server with certificate which has incorrect CN and missing SAN.</li> <li>• Attempt the connection from the TOE to the TLS Server.</li> <li>• Verified with log that connection the TOE was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul>
<b>Expected Test Results</b>	The TOE does not connect to a server when the presented certificate has an invalid CN and missing SAN
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects the connection if the server certificate has an incorrect reference identifier type for IPv4, IPv6, or FQDN in the CN field and lacks SAN.
<b>Result</b>	Pass

### 7.7.13 FCS\_DTLS\_EXT.1.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 2 [conditional]: The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When</p>

	<p>testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.</p>
<p><b>Note</b></p>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p>a) <i>DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i>  <i>Or:</i>  b) <i>DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<p><b>Test Steps</b></p>	<p><b><u>Part 1 - IPV4</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv4.</li> <li>• Create a certificate with correct CN and incorrect SAN.</li> <li>• Start the TLS server with certificate which has correct CN and incorrect SAN.</li> <li>• Attempt the connection from TOE to the TLS server.</li> <li>• Verified with log that connection the TOE will successful if the SAN is wrong because SAN is not claimed.</li> <li>• Verified with Wireshark that connection was accepted.</li> </ul> <p><b><u>Part 2 – IPv6</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv6.</li> <li>• Create a certificate with correct CN and incorrect SAN.</li> <li>• Start the TLS server with certificate which has correct CN and incorrect SAN.</li> <li>• Attempt the connection from TOE to the TLS server.</li> <li>• Verified with log that connection the TOE was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul>

	<p><b>Part 3 – FQDN</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as FQDN.</li> <li>• Create the Server certificate showing correct CN and incorrect SAN.</li> <li>• Start the TLS server with certificate which has correct CN and incorrect SAN.</li> <li>• Attempt the connection from the TOE to the TLS Server.</li> <li>• Verified with log that connection the TOE was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul>
<b>Expected Test Results</b>	The TOE rejects any connection where the CN is correct, and SAN is incorrect
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects the connection if the server certificate has an correct reference identifier type for IPv4, IPv6, or FQDN in the CN field and incorrect SAN.
<b>Result</b>	Pass

### 7.7.14 FCS\_DTLS\_EXT.1.2 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 3 [conditional]: If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this test shall be omitted.</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></p> <p><i>Or:</i></p> <p><i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p>



	<ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Test Steps</b>	<p><b><u>Part 1 - IPv4</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv4</li> <li>• Create a Server certificate with correct CN and missing SAN</li> <li>• Start the TLS server with certificate which has correct CN and missing SAN</li> <li>• Attempt the connection from TOE to the TLS server</li> <li>• Verify with log that connection was successful.</li> <li>• Verify with Wireshark that connection was successful.</li> </ul> <p><b><u>Part 2 – IPv6</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv6</li> <li>• Create a Server certificate with correct CN and missing SAN</li> <li>• Start the TLS server with a certificate which has correct CN and missing SAN</li> <li>• Attempt the connection from TOE to the TLS server</li> <li>• Verify with log that connection was successful.</li> <li>• Verify with Wireshark that connection was successful.</li> </ul> <p><b><u>Part 3 – FQDN</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as FQDN</li> <li>• Create a Server certificate with correct CN and missing SAN</li> <li>• Start the TLS server with certificate which has correct CN and missing SAN</li> <li>• Attempt the connection from TOE to the TLS server</li> <li>• Verify with log that connection was successful.</li> <li>• Verify with Wireshark that connection was successful.</li> </ul>
<b>Expected Test Results</b>	The TOE successfully connects when there a valid CN and no SAN present in the certificate
<b>Pass/Fail with Explanation</b>	Pass. A connection was established when TOE is presented with a server certificate which contains a CN that matches the reference identifier type for IPv4, IPv6, or FQDN and does not contain the SAN extension. This meets the testing requirements.
<b>Result</b>	Pass

## 7.7.15 FCS\_DTLS\_EXT.1.2 Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 4 [conditional]: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <ul style="list-style-type: none"> <li><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></li> <li><i>Or:</i></li> <li><i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></li> </ul> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li><i>• IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Test Steps</b>	<p><b><u>Part 1 - IPv4</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv4</li> <li>• Create a Server certificate with incorrect CN and valid SAN</li> <li>• Start the TLS server with certificate which has incorrect CN and valid SAN</li> <li>• Attempt the connection from TOE to the TLS server</li> <li>• Verify with log that connection was successful.</li> <li>• Verify with Wireshark that connection was successful.</li> </ul> <p><b><u>Part 2 – IPv6</u></b></p>

	<ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as IPv6</li> <li>• Create a Server certificate with incorrect CN and valid SAN</li> <li>• Start the TLS server with certificate which has incorrect CN and valid SAN</li> <li>• Attempt the connection from TOE to the TLS server</li> <li>• Verify with log that connection was successful.</li> <li>• Verify with Wireshark that connection was successful.</li> </ul> <p><b>Part 3 – FQDN</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for reference identifier name as FQDN</li> <li>• Create a Server certificate with incorrect CN and valid SAN</li> <li>• Start the TLS server with a certificate which has incorrect CN and valid SAN</li> <li>• Attempt the connection from TOE to the TLS server</li> <li>• Verify with log that connection was successful.</li> <li>• Verify with Wireshark that connection was successful.</li> </ul>
<b>Expected Test Results</b>	The TOE successfully connects when there is an invalid CN and valid SAN
<b>Pass/Fail with Explanation</b>	Pass. A connection was established when TOE is presented with a server certificate that contains a CN that does not match the reference identifier type for IPv4, IPv6, or FQDN but does contain an identifier in the SAN that matches. This meets the testing requirements.
<b>Result</b>	Pass

### 7.7.16 FCS\_DTLSC\_EXT.1.2 Test #5 (1)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID):</p> <ol style="list-style-type: none"> <li>1) [conditional]: The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.</li> </ol>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <ol style="list-style-type: none"> <li>a) <i>DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></li> </ol> <p><i>Or:</i></p> <ol style="list-style-type: none"> <li>b) <i>DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></li> </ol>

	<p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li><i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> <li><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></li> </ul>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a certificate containing a wildcard that is not in the left-most label of the presented identifier as CN-ID with DNS</li> <li>• Start TLS server with certificate containing a wildcard that is not in the left-most label of the presented identifier</li> <li>• Attempt the connection from TOE to the TLS server using reference identifier</li> <li>• Verify with Wireshark that connection was rejected</li> <li>• Verify with log that connection was rejected</li> </ul>
<b>Expected Test Results</b>	The TOE denies any connection where a wildcard is present
<b>Pass/Fail with Explanation</b>	Pass. TOE rejects the connection when the reference identifier with single left-most labels is presented in the certificate. This meets the testing requirements.
<b>Result</b>	Pass

### 7.7.17 FCS\_DTLSC\_EXT.1.2 Test #5 (2)(a)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID):</p>

	<p>2) The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com).</p> <p>The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds, if wildcards are supported, or fails if wildcards are not supported.</p> <p>(Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)</p>
<p><b>Note</b></p>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p>a) <i>DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></p> <p><i>Or:</i></p> <p>b) <i>DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<p><b>Test Steps</b></p>	<ul style="list-style-type: none"> <li>• Create a server certificate containing a wildcard in the left-most label of the presented identifier as CN-ID with DNS</li> <li>• Start TLS server with certificate containing a wildcard in the left-most label.</li> <li>• Attempt the connection from TOE to the TLS server using reference identifier with a single left-most label.</li> <li>• Verified with Wireshark that connection was successful.</li> <li>• Verified with logs that connection was successful.</li> </ul>
<p><b>Expected Test Results</b></p>	<p>The TOE denies any connection where a wildcard is present</p>

<b>Pass/Fail with Explanation</b>	Pass. The connection was Unsuccessful when the evaluator presented a server certificate containing a wildcard in the left-most label as the TOE does not support Wildcards.
<b>Result</b>	Pass

### 7.7.18 FCS\_DTLSC\_EXT.1.2 Test #5 (2)(b)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID):</p> <ol style="list-style-type: none"> <li>2) The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com).</li> </ol> <p>The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails.</p> <p>(Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <ol style="list-style-type: none"> <li>a) <i>DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></li> </ol> <p><i>Or:</i></p> <ol style="list-style-type: none"> <li>b) <i>DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></li> </ol> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul>

	<i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a server certificate containing a wildcard in the left-most label of the presented identifier as CN-ID with DNS</li> <li>• Start the TLS server with certificate containing a wildcard in the left-most label</li> <li>• Attempt the connection from TOE to the TLS server using reference identifier without a left-most label as in the certificate</li> <li>• Verified with Wireshark that connection failed</li> <li>• Verify connection failed via log</li> </ul>
<b>Expected Test Results</b>	The TOE denies any connection where a wildcard is present
<b>Pass/Fail with Explanation</b>	Pass. The connection failed when the evaluator presented a server certificate containing a wildcard in the left-most label and configured the reference identifier without a left-most label.
<b>Result</b>	Pass

### 7.7.19 FCS\_DTLS\_EXT.1.2 Test #5 (2)(c)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID):</p> <p>2) The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com).</p> <p>The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.</p> <p>(Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></p> <p><i>Or:</i></p> <p><i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p>

	<p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li><i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Test Steps &amp;</b>	<ul style="list-style-type: none"> <li>• Create a server certificate containing a wildcard in the left-most label of the presented identifier as CN-ID with DNS.</li> <li>• Start the TLS server with certificate containing a wildcard in the left-most label.</li> <li>• Attempt the connection from TOE to the TLS server using reference identifier with two left-most labels.</li> <li>• Verified with Wireshark that connection failed.</li> <li>• Verify connection failed via log.</li> </ul>
<b>Expected Test Results</b>	The TOE denies any connection where a wildcard is present
<b>Pass/Fail with Explanation</b>	Pass. The connection failed when the evaluator presented a server certificate containing a wildcard in the left-most label and configured.
<b>Result</b>	Pass

### 7.7.20 FCS\_DTLSC\_EXT.1.2 Test #6

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Objective: The objective of this test is to ensure the TOE is able to differentiate between IP address identifiers that are not allowed to contain wildcards and other types of identifiers that may contain wildcards.</p>



	<p>Test 6: [conditional] If IP address identifiers are supported in the SAN or CN, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with a wildcard asterisk (*)</p> <p>(e.g. CN=*.168.0.1 when connecting to 192.168.0.1, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g. IPv4, IPv6).</p> <p>Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 6.</p> <p><b>TD0790 has been applied.</b></p>
<p><b>Note</b></p>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <ul style="list-style-type: none"> <li><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></li> <li><i>Or:</i></li> <li><i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></li> </ul> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<p><b>Test Steps</b></p>	<p><b>Part 1 - IPv4</b></p> <ul style="list-style-type: none"> <li>• Create a certificate with incorrect CN and missing SAN.</li> <li>• Start the TLS server with certificate which has incorrect CN and missing SAN.</li> <li>• Attempt the connection from TOE to the TLS server.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verified with log that connection was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul> <p><b>Part 2 – IPv6</b></p> <ul style="list-style-type: none"> <li>• Create a certificate with incorrect CN and missing SAN.</li> <li>• Start the TLS server with certificate which has incorrect CN and missing SAN.</li> <li>• Attempt the connection from TOE to the TLS server.</li> <li>• Verified with log that connection was rejected.</li> <li>• Verified with Wireshark that connection was rejected.</li> </ul>
<b>Expected Test Results</b>	The TOE denies any connection where a wildcard is present
<b>Pass/Fail with Explanation</b>	Pass. The evaluator has presented a server certificate that contains a CN that matches the reference identifier where one of the groups in IP address (IPv4 and IPv6) has been replaced with an asterisk (*) and missing the SAN extension and verified that the connection failed.
<b>Result</b>	Pass

#### 7.7.21 FCS\_DTLSC\_EXT.1.2 Test #7a

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 7: [conditional] If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):</p> <ol style="list-style-type: none"> <li>1) The evaluator shall present a server certificate that does not contain an identifier in the Subject (DN) attribute type(s) that matches the reference identifier. The evaluator shall verify that the connection fails.</li> </ol>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <ol style="list-style-type: none"> <li>a) <i>DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i></li> </ol> <p><i>Or:</i></p> <ol style="list-style-type: none"> <li>b) <i>DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></li> </ol>

	<p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Pass/Fail with Explanation</b>	NA, TOE does not use FPT_ITT for Secure channel.

### 7.7.22 FCS\_DTLSC\_EXT.1.2 Test #7b

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 7: [conditional] If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):</p> <ol style="list-style-type: none"> <li>2) The evaluator shall present a server certificate that contains a valid identifier as an attribute type other than the expected attribute type (e.g. if the TOE is configured to expect id-at-serialNumber=correct_identifier, the certificate could instead include id-at-name=correct_identifier), and does not contain the SAN extension. The evaluator shall verify that the connection fails. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass this test.</li> </ol>

<p><b>Note</b></p>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p>a) <i>DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i>  <i>Or:</i></p> <p>b) <i>DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li>• <i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<p><b>Pass/Fail with Explanation</b></p>	<p>NA, TOE does not use FPT_ITT for Secure channel.</p>

**7.7.23 FCS\_DTLSC\_EXT.1.2 Test #7c**

Item	Data
<p><b>Test Assurance Activity</b></p>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 7: [conditional] If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):</p>

	<p>3) The evaluator shall present a server certificate that contains a Subject attribute type that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds.</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i>  <i>Or:</i>  <i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li><i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Pass/Fail with Explanation</b>	<p>NA, TOE does not use FPT_ITT for Secure channel.</p>

#### 7.7.24 FCS\_DTLSC\_EXT.1.2 Test #7d

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a DTLS connection:</p> <p>Test 7: [conditional] If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):</p>

	<p>4) The evaluator shall confirm that all use of wildcards results in connection failure regardless of whether the wildcards are used in the left or right side of the presented identifier. (Remark: Use of wildcards is not addressed within RFC 5280.)</p>
<b>Note</b>	<p><i>Note that tests 1-6 are only applicable to:</i></p> <p><i>a) DTLS-based trusted channel communications according to FTP_ITC.1 and trusted path communications according to FTP_TRP.1</i>  <i>Or:</i>  <i>b) DTLS-based trusted channel communications when RFC 6125 is selected for FPT_ITT.1</i></p> <p><i>Test 7 is only applicable to DTLS-based trusted channel communications when RFC 5280 is selected for FPT_ITT.1. Therefore, all tests are marked as conditional. Note that for some tests additional conditions apply.</i></p> <p><i>IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:</i></p> <ul style="list-style-type: none"> <li><i>IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.</i></li> </ul> <p><i>IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested..</i></p>
<b>Pass/Fail with Explanation</b>	<p>NA, TOE does not use FPT_ITT for Secure channel.</p>

### 7.7.25 FCS\_DTLSC\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows:</p> <p>Test 1: Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.</p>

<b>Pass/Fail with Explanation</b>	Pass. This test is covered as a part of FIA_X509_EXT.1.1 Test #1.
<b>Result</b>	Pass

### 7.7.26 FCS\_DTLSC\_EXT.1.3 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows:</p> <p>Test 2: The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.</p>
<b>Pass/Fail with Explanation</b>	<p>This Test is covered by FCS_DTLSC_EXT.1.2 Test #1 (failed matching of the reference identifier), FIA_X509_EXT.1.1/Rev Test #1(a)&amp;(b) (failed validation of the certificate path), FIA_X509_EXT.1.1/Rev Test #2 (failed validation of the expiration date) and FIA_X509_EXT.2 Test #1 (failed determination of revocation status) FCS_TLSC_EXT.1.2 Test #1, FIA_X509_EXT.1.1/Rev Test #1(a)&amp;(b) and FIA_X509_EXT.1.1/Rev Test #3. This meets the testing requirements.</p>
<b>Result</b>	Pass

### 7.7.27 FCS\_DTLSC\_EXT.1.3 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows:</p> <p>Test 3: The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. If any override mechanism is defined for failed certificate validation, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate</p>

	validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
<b>Pass/Fail with Explanation</b>	Pass. This Test covered by DTLSC_EXT.1.1 Test #2 (inappropriate value in the EKU field) where server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. This meets the testing requirements
<b>Result</b>	Pass

#### 7.7.28 FCS\_DTLSC\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1 [conditional]: If the TOE presents the Supported Elliptic Curves/Supported Groups Extension, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.
<b>Pass/Fail with Explanation</b>	NA, TOE does not support Elliptic Curves or Group Extension

#### 7.7.29 FCS\_DTLSC\_EXT.2.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall establish a connection to a peer server that is configured for mutual authentication (i.e. sends a server Certificate Request (type 13) message). The evaluator observes that the TOE DTLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages during its negotiation of a DTLS channel and that Application Data is sent.</p> <p>In addition, all other testing in FCS_DTLSC_EXT.1 and FIA_X509_EXT.* must be performed as per the requirements.</p> <p><b>TD0670 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Initiate a connection with the TOE over DTLS connection to a peer server that is configured for mutual authentication for successful connection.</li> <li>• Verify the connection via packet capture &amp; observe Server send a server Certificate Request (type 13) message.</li> <li>• Observe TOE DTLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages.</li> </ul>



<b>Expected Test Results</b>	The TOE properly executes the mutually authenticated DTLS connection
<b>Pass/Fail with Explanation</b>	Pass, the evaluator has presented a Peer server certificate for mutual authentication & verifies server certificate requests also client certificate verify with the supported type for successful connection. This meets the Testing requirements.
<b>Result</b>	Pass

### 7.7.30 FCS\_DTLSC\_EXT.2.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall establish a DTLS connection. The evaluator will then modify at least one byte in a record message and verify that the Client discards the record or terminates the DTLS session.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Upload a valid certificate on the TOE.</li> <li>• Initiate a connection from the TOE to the DTLS server and show the connection being successful.</li> <li>• Note the record message data of the DTLS server that is to be modified.</li> <li>• Pass the previously noted fixed bytes, offset and new data bytes for the AcumenMITM tool to replace the bytes in the record data of the certificate.</li> <li>• Setup a server listening to allow DTLS connection on port 5001.</li> <li>• Initiate a DTLS connection from the TOE to the DTLS server.</li> <li>• Verify that the modification happens and the DTLS connection fails.</li> <li>• Verify the DTLS connection failure via TOE's logs.</li> <li>• Verify the DTLS connection failure via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the DTLS connection with the server containing modified record data in its certificate.
<b>Pass/Fail with Explanation</b>	Pass. The TOE terminates the DTLS connection with the server having modified record data in its certificate.
<b>Result</b>	Pass

### 7.7.31 FCS\_DTLSC\_EXT.2.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall set up a DTLS connection with a DTLS Server. The evaluator shall then capture traffic sent from the DTLS Server to the TOE. The evaluator shall retransmit copies of this traffic to the TOE in order to impersonate the DTLS Server. The evaluator shall observe that the TSF

	does not take action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Upload a complete certificate validation chain on the TOE.</li> <li>• Establish a successful connection with the DTLS server from the TOE.</li> <li>• Verify the successful connection via packet capture.</li> <li>• Verify the logs for the successful connection.</li> <li>• Segregate just the traffic captured from the DTLS server.</li> <li>• Retransmit the previous captured traffic of the successful DTLS connection to the TOE in order to impersonate the DTLS Server.</li> <li>• Verify the unsuccessful DTLS connection via TOE's log.</li> <li>• Verify that the TOE does not respond to the impersonated DTLS server via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should not take any action in response to receiving replay traffic from the impersonated server and the TOE'S audit log should indicate that the replayed traffic was discarded.
<b>Pass/Fail with Explanation</b>	Pass. The evaluator has verified TOE does not take action in response to retransmitted traffic and that the audit log indicates that the replayed traffic was discarded.
<b>Result</b>	Pass

## 7.8 SSHC

### 7.8.1 FCS\_SSHC\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: For each claimed public-key authentication method, the evaluator shall configure the TOE to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH server to demonstrate the use of all claimed public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test.</p> <p><b>TD0636 has been implemented</b></p>
<b>Test Steps</b>	<p>SSH-RSA</p> <ul style="list-style-type: none"> <li>• Show the SSH-RSA public key generated on the TOE and move it over to the syslog server.</li> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul> <p>ECDSA-sha2-nistp256</p> <ul style="list-style-type: none"> <li>• Show the ECDSA-SHA2-NISTP256 public key generated on the TOE and move it over to the syslog server.</li> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul>

	<p>ECDSA-sha2-nistp384</p> <ul style="list-style-type: none"> <li>• Show the ECDSA-SHA2-NISTP384 public key generated on the TOE and move it over to the syslog server.</li> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow successful connections with all 3 public keys.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful connection with all 3 public key algorithms.
<b>Result</b>	Pass

### 7.8.2 FCS\_SSHC\_EXT.1.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: [Conditional] If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then following the guidance documentation the evaluator shall configure the TOE to perform password-based authentication with a remote SSH server to demonstrate that the TOE can successfully authenticate using a password as an authentication method.</p> <p><b>TD0636 has been implemented.</b></p>
<b>Pass/Fail with Explanation</b>	N/A. The ST does not select password-based authentication method for SSHC.

### 7.8.3 FCS\_SSHC\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	If a packet is sent that is larger than the regular specified packet, the TOE should drop it.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully drops a packet that is larger than the specified size.
<b>Result</b>	Pass

### 7.8.4 FCS\_SSHC\_EXT.1.4 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.</p> <p>To verify this, the evaluator shall start session establishment for an SSH connection with a remote server (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS.</p> <p>The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• Verify that the SSH session was encrypted using only the claimed cipher(s) via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow a successful connection with all the claimed ciphers.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully allows connections with the specified ciphers.
<b>Result</b>	Pass

### 7.8.5 FCS\_SSHC\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE.</p> <p>It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p>Test objective: The purpose of this positive test is to check the authentication of the server by the client (when establishing the transport layer connection), and not for checking generation of the authentication message from the client (in the User Authentication Protocol). The evaluator shall therefore establish sufficient separate SSH connections (with an appropriately configured server) to cause the TOE to demonstrate use of all public key algorithms claimed in FCS_SSHC_EXT.1.5 in the ST.</p>
<b>Test Steps</b>	<p>SSH-RSA</p> <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul> <p>ECDSA-sha2-nistp256</p> <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul> <p>ECDSA-sha2-nistp384</p>

	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow an SSH connection to be successful to an external server.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful connection with all 3 public key algorithms.
<b>Result</b>	Pass

### 7.8.6 FCS\_SSHC\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall configure an SSH server to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected.
<b>Test Steps</b>	SSH-DSS <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> <li>• The evaluator displays log evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow any traffic to be passed since the public key algorithm is not supported.
<b>Pass/Fail with Explanation</b>	The TOE does not allow any traffic to be passed since the host public key is not supported.

### 7.8.7 FCS\_SSHC\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	[conditional, if an <b>HMAC or AEAD_AES*_GCM</b> algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except “implicit”, specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
<b>Test Steps</b>	HMAC-SHA1 <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> <li>• The evaluator shows log evidence of the connection attempt.</li> </ul> HMAC-SHA2-256 <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> <li>• The evaluator shows log evidence of the connection attempt.</li> </ul> HMAC-SHA2-512 <ul style="list-style-type: none"> <li>• The evaluator attempts a connection to the syslog server.</li> </ul>

	<ul style="list-style-type: none"> <li>The evaluator shows packet capture evidence of the connection attempt.</li> <li>The evaluator shows log evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow connections using all 3 mac algorithms.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows successful connections using all 3 mac algorithms.
<b>Result</b>	Pass

### 7.8.8 FCS\_SSHC\_EXT.1.6 Test #2

Item	Data
<b>Test Assurance Activity</b>	[conditional, if an <b>HMAC or AEAD_AES*_GCM</b> algorithm is selected in the ST] The evaluator shall configure an SSH server to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt fails Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
<b>Test Steps</b>	HMAC-MD5 <ul style="list-style-type: none"> <li>The evaluator attempts a connection to the syslog server.</li> <li>The evaluator shows packet capture evidence of the connection attempt.</li> <li>The evaluator shows log evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow a connection with an unsupported mac algorithm.
<b>Pass/Fail with Explanation</b>	The TOE successfully does not allow a connection using an unsupported mac algorithm.
<b>Result</b>	Pass

### 7.8.9 FCS\_SSHC\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure an SSH server to permit all allowed key exchange methods. The evaluator shall attempt to connect from the TOE to the SSH server using each allowed key exchange method and observe that each attempt succeeds.
<b>Test Steps</b>	Diffie-hellman-group14-sha1 <ul style="list-style-type: none"> <li>Configure the SSH Server for the allowed key exchange method diffie-hellman-group14-sha1.</li> <li>The evaluator attempts a connection to the syslog server.</li> <li>The evaluator shows log evidence of the connection attempt.</li> <li>The evaluator shows packet capture evidence of the connection attempt.</li> </ul> Ecdh-sha2-nistp256 <ul style="list-style-type: none"> <li>Configure the SSH Server for the allowed key exchange method ecdh-sha2-nistp256.</li> <li>The evaluator attempts a connection to the syslog server.</li> <li>The evaluator shows log evidence of the connection attempt.</li> </ul>

	<ul style="list-style-type: none"> <li>The evaluator shows packet capture evidence of the connection attempt.</li> </ul> <p>Ecdh-sha2-nistp384</p> <ul style="list-style-type: none"> <li>Configure the SSH Server for the allowed key exchange method ecdh-sha2-nistp384.</li> <li>The evaluator attempts a connection to the syslog server.</li> <li>The evaluator shows log evidence of the connection attempt.</li> <li>The evaluator shows packet capture evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow connections using all 3 key exchange methods.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows successful connections using all 3 key exchange methods.
<b>Result</b>	Pass

### 7.8.10 FCS\_SSHC\_EXT.1.8 Test #1t

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the <b>time-based</b> threshold and the traffic-based threshold.</p> <p>For testing of the time-based threshold, the evaluator shall use the TOE to connect to an SSH server and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time, but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH server the TOE is connected to.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>The evaluator attempts a connection where the testing tool sends data for 60 minutes in order trigger an ssh rekey.</li> <li>The evaluator shows packet capture evidence of the connection attempt.</li> <li>The evaluator shows log evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	The TOE should perform an SSH rekey after the configured time period has passed.
<b>Pass/Fail with Explanation</b>	Pass, The TOE sends a successful rekey request after the configured amount of time elapsed.
<b>Result</b>	Pass

### 7.8.11 FCS\_SSHC\_EXT.1.8 Test #1b

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the <b>traffic-based</b> threshold.</p> <p>For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH server and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHC_EXT.1.8).</p> <p>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic, but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH server the TOE is connected to.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p> <p>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:</p> <ol style="list-style-type: none"> <li>1) An argument is present in the TSS Section describing this hardware- based limitation and</li> <li>2) All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts a connection where the testing tool sends 1GB of data in order trigger an ssh rekey.</li> <li>• The evaluator shows packet capture evidence of the connection attempt.</li> <li>• The evaluator shows log evidence of the connection attempt.</li> </ul>
<b>Expected Test Results</b>	<p>The TOE should perform an SSH re-key after the configured data limit has been reached.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass, The TOE sends a successful rekey request after the configured amount of data has been elapsed.</p>
<b>Result</b>	<p>Pass</p>



### 7.8.12 FCS\_SSHC\_EXT.1.9 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall delete all entries in the TOE's list of recognized SSH server host keys and, if selected, all entries in the TOE's list of trusted certification authorities. The evaluator shall initiate a connection from the TOE to an SSH server. The evaluator shall ensure that the TOE either rejects the connection or displays the SSH server's public key (either the key bytes themselves or a hash of the key using any allowed hash algorithm) and prompts the Security Administrator to accept or deny the key before continuing the connection.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Delete all know-host entries in the TOE's SSH configuration.</li> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• Verify the unsuccessful connection using TOE logs.</li> <li>• Verify the unsuccessful connection using Packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Remove all entries Know host entries from SSH configuration of the TOE.</li> <li>• SSH connection attempt from TOE would be rejected.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass, The TOE rejects the SSH connection when the host key of Server is not present.
<b>Result</b>	Pass

### 7.8.13 FCS\_SSHC\_EXT.1.9 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key.</p> <p>If 'password-based' is selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords).</p> <p>If 'password-based' is not selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using public key-based authentication and shall ensure that the TOE rejects the connection.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Load the SSH server hostkey into the TOE's local database.</li> <li>• Change the SSH server hostkey pair without loading it into the TOE.</li> <li>• The evaluator attempts a connection to the syslog server.</li> <li>• Verify the unsuccessful connection using TOE logs.</li> <li>• Verify the unsuccessful connection using Packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the connection to SSH server when there is a mismatch in the public key.</li> <li>• Verify the failed connection using TOE logs.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass, The TOE rejects the connection to the SSH server when there is a mismatch in the public key.
<b>Result</b>	Pass

## 7.9 SHSS

### 7.9.1 FCS\_SSHS\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test objective: The purpose of these tests is to verify server supports each claimed client authentication method.</p> <p>Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<p><b>SSH-RSA</b></p> <ul style="list-style-type: none"> <li>• Generate the SSH-RSA key on the VM.</li> <li>• Configure the TOE to support SSH-RSA based SSH authentication method.</li> <li>• Log into the TOE using SSH with SSH-RSA based authentication.</li> <li>• Verify the successful connection using logs on TOE.</li> <li>• Verify the successful connection using packet capture.</li> </ul> <p><b>ECDSA-SHA2-NISTP256</b></p> <ul style="list-style-type: none"> <li>• Generate the ECDSA-SHA2-NISTP256 key on the VM.</li> <li>• Configure the TOE to support ECDSA-SHA2-NISTP256 based SSH authentication method.</li> <li>• Log into the TOE using SSH with ECDSA-SHA2-NISTP256 based authentication.</li> <li>• Verify the successful connection using logs on TOE.</li> <li>• Verify the successful connection using packet capture.</li> </ul> <p><b>ECDSA-SHA2-NISTP384</b></p> <ul style="list-style-type: none"> <li>• Generate the ECDSA-SHA2-NISTP384 key on the VM.</li> <li>• Configure the TOE to support ECDSA-SHA2-NISTP384 based SSH authentication method.</li> <li>• Log into the TOE using SSH with ECDSA-SHA2-NISTP384 based authentication.</li> <li>• Verify the successful connection using logs on TOE.</li> <li>• Verify the successful connection using packet capture.</li> </ul>
<b>Expected Test Results</b>	<p>The TOE must successfully establish a SSH session connection with the client using all the claimed public key algorithms.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass, The TOE accepts SSH connections with the claimed public key algorithm.</p>
<b>Result</b>	<p>Pass</p>

### 7.9.2 FCS\_SSHS\_EXT.1.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the SSH client with a new RSA keypair for SSH without configuring the TOE and attempt to login using ssh-rsa key.</li> <li>• Log into the TOE via SSH using RSA-based authentication.</li> <li>• Verify authentication logs on TOE.</li> <li>• Verify authentication failure via packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject SSH connections when incorrect/unknown public keys are presented.
<b>Pass/Fail with Explanation</b>	Pass, The TOE denied a connection with a remote SSH user when incorrect authentication credentials are presented.
<b>Result</b>	Pass

### 7.9.3 FCS\_SSHS\_EXT.1.2 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator logs into the TOE via SSH with password authentication.</li> <li>• The evaluator displays authentication logs.</li> <li>• The evaluator displays packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow a successful connection to the TOE.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful connection from the evaluator.
<b>Result</b>	Pass

#### 7.9.4 FCS\_SSHS\_EXT.1.2 Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator logs into the TOE using SSH with the incorrect password for authentication.</li> <li>• The evaluator displays authentication logs.</li> <li>• The evaluator displays packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow a successful connection using incorrect login credentials.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow a successful connection using incorrect credentials.
<b>Result</b>	Pass

#### 7.9.5 FCS\_SSHS\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator uses a special tool to send abnormally large packets.</li> <li>• The evaluator verifies that when a large packet is received the connection is dropped using packet capture evidence.</li> <li>• The evaluator verifies the logs reflect the dropped packet.</li> </ul>
<b>Expected Test Results</b>	The TOE should lose connection due to receiving a packet larger than specified.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully declines the connection as the TOE receives an abnormally large packet.
<b>Pass</b>	Pass

#### 7.9.6 FCS\_SSHS\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.

	<p>To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test.</p> <p>If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator establishes a connection to the TOE using the encryption algorithm aes128-cbc.</li> <li>• The evaluator verifies the connection attempt with audit log evidence.</li> <li>• The evaluator verifies AES128-cbc was used with packet capture evidence.</li> <li>• The evaluator verifies that all ciphers claimed in the ST are supported by the TOE using the Packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow the evaluator to authenticate using all of the supported ciphers.
<b>Pass/Fail with Explanation</b>	Pass, The TOE is able to establish a SSH session with the client successfully using only the claimed encryption algorithms.
<b>Result</b>	Pass

### 7.9.7 FCS\_SSHS\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p><b>TD0631 has been applied</b></p>
<b>Test Steps</b>	<p>SSH-RSA</p> <ul style="list-style-type: none"> <li>• The evaluator generates a public key for the TOE.</li> <li>• The evaluator attempts a connection with the newly generated public key.</li> <li>• The evaluator shows log evidence of a successful connection.</li> <li>• The evaluator documents the key exchange between the client and the SSH server using packet capture evidence.</li> </ul> <p>ECDSA-SHA2-NISTP256</p> <ul style="list-style-type: none"> <li>• The evaluator generates a public key for the TOE.</li> <li>• The evaluator attempts a connection with the newly generated public key.</li> </ul>

	<ul style="list-style-type: none"> <li>The evaluator shows log evidence of a successful connection.</li> <li>The evaluator documents the key exchange between the client and the SSH server using packet capture evidence.</li> </ul> <p>ECDSA-SHA2-NISTP384</p> <ul style="list-style-type: none"> <li>The evaluator generates a public key for the TOE.</li> <li>The evaluator attempts a connection with the newly generated public key.</li> <li>The evaluator shows log evidence of a successful connection.</li> <li>The evaluator documents the key exchange between the client and the SSH server using packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow a successful connection using the configured public keys.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully authenticates using all 3 public key types.
<b>Result</b>	Pass

### 7.9.8 FCS\_SSHS\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected. <b>TD0631 has been applied</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>The evaluator creates a connection to the TOE using a public key algorithm that is not supported by the ST.</li> <li>The evaluator makes a connection attempt to the TOE using an unsupported public key algorithm.</li> <li>The evaluator verifies that the connection rejection with packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow an SSH connection when using an unsupported public key algorithm.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully declines the login using the configured public key.
<b>Result</b>	Pass

### 7.9.9 FCS\_SSHS\_EXT.1.6 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>Test 1: [conditional, if an <b>HMAC or AEAD_AES*_GCM</b> algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except “implicit”, specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p>Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.</p>
<b>Test Steps</b>	<p>The evaluator configures the TOE to support the algorithms specified in the ST: hmac-sha1, hmac-sha2-256, hmac-sha2-512.</p> <p><b>HMAC-SHA1</b></p> <ul style="list-style-type: none"> <li>• The evaluator establishes an SSH session with the configured supported algorithms (HMAC-SHA1).</li> <li>• The evaluator verifies that HMAC-SHA1 algorithm is the intended algorithm used with log file evidence.</li> <li>• The evaluator verifies that HMAC-SHA1 algorithm is the intended algorithm used with packet capture evidence.</li> </ul> <p><b>HMAC-SHA2-256</b></p> <ul style="list-style-type: none"> <li>• The evaluator establishes an SSH session with the configured supported algorithms (HMAC-SHA2-256).</li> <li>• The evaluator verifies that HMAC-SHA2-256 algorithm is the intended algorithm used with log file evidence.</li> <li>• The evaluator verifies that HMAC-SHA2-256 algorithm is the intended algorithm used with packet capture evidence.</li> </ul> <p><b>HMAC-SHA2-512</b></p> <ul style="list-style-type: none"> <li>• The evaluator establishes an SSH session with the configured supported algorithms (HMAC-SHA2-512).</li> <li>• The evaluator verifies that HMAC-SHA2-512 algorithm is the intended algorithm used with log file evidence.</li> <li>• The evaluator verifies that HMAC-SHA2-512 algorithm is the intended algorithm used with packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	<p>The TOE should allow successful authentication with the configured message authentication algorithms.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass, The TOE successfully allows connections with all 3 message authentication algorithms.</p>
<b>Result</b>	<p>Pass</p>

### 7.9.10 FCS\_SSHS\_EXT.1.6 Test #2

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>Test 2: [conditional, if an <b>HMAC or AEAD_AES*_GCM</b> algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.</p> <p>Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts to establish an SSH connection to the TOE.</li> <li>• The evaluator verifies using audit logs that the connection attempt was unsuccessful.</li> <li>• The evaluator verifies using packet capture evidence that the TOE does not continue negotiation.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the connection as the unsupported algorithm is used for negotiation.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully declines the connection with an unsupported mac.
<b>Result</b>	Pass

#### 7.9.11 FCS\_SSHS\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts to establish a connection from an SSH client using diffiehellman-group1-sha1 as the key exchange method.</li> <li>• The evaluator captures the traffic between the ssh client and the ssh server.</li> <li>• The evaluator verifies that the session was not established using an unsupported key exchange method.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the connection as the key exchange algorithm used for the connection is not supported.
<b>Pass/Fail with Explanation</b>	Pass, The TOE does not allow a successful connection using the key exchange method Diffie-hellman-group1-sha1.
<b>Result</b>	Pass

#### 7.9.12 FCS\_SSHS\_EXT.1.7 Test #2

Item	Data
------	------



<b>Test Assurance Activity</b>	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
<b>Test Steps</b>	<p>Diffie-hellman-group14-sha1</p> <ul style="list-style-type: none"> <li>• The evaluator logs in over the SSH connection with the SSH testing tool using the new key exchange method.</li> <li>• The evaluator documents the connection attempt with log evidence from the TOE.</li> <li>• The evaluator documents the key exchange between the client and the SSH server using packet capture evidence.</li> </ul> <p>ECDH-SHA2-NISTP256</p> <ul style="list-style-type: none"> <li>• The evaluator logs in over the SSH connection with the SSH testing tool using the new key exchange method.</li> <li>• The evaluator documents the connection attempt with log evidence from the TOE.</li> <li>• The evaluator documents the key exchange between the client and the SSH server using packet capture evidence.</li> </ul> <p>ECDH-SHA2-NISTP384</p> <ul style="list-style-type: none"> <li>• The evaluator logs in over the SSH connection with the SSH testing tool using the new key exchange method.</li> <li>• The evaluator documents the connection attempt with log evidence from the TOE.</li> <li>• The evaluator documents the key exchange between the client and the SSH server using packet capture evidence.</li> </ul>
<b>Expected Test Results</b>	The TOE should allow a successful connection using each selected key exchange method.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows a successful connection using each selected key exchange algorithms.
<b>Result</b>	Pass

### 7.9.13 FCS\_SSHS\_EXT.1.8 Test #1t

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the <b>time-based threshold</b> and the traffic-based threshold.</p> <p>For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour.</p>

	<p>The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Run acumen-sshs tool and wait for 1 hour for the rekey to occur based on time.</li> <li>• The evaluator waits 60 minutes for the re-key to occur.</li> </ul>
<b>Expected Test Results</b>	The TOE should perform an SSH rekey after the configured time period has passed.
<b>Pass/Fail with Explanation</b>	Pass, The TOE sends a successful rekey request after the configured amount of time elapsed.
<b>Result</b>	Pass

#### 7.9.14 FCS\_SSHS\_EXT.1.8 Test #1b

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the <b>traffic-based</b> threshold.</p> <p>For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8).</p> <p>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p>

	<p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p> <p>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:</p> <ol style="list-style-type: none"> <li>1. An argument is present in the TSS Section describing this hardware- based limitation and</li> <li>2. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Run acumen-sshs tool to transfer 1 GB file and wait for the rekey to occur based on the configured data threshold.</li> <li>• The evaluator waits for 1GB file to transfer for the re-key to occur based on the configured data threshold.</li> </ul>
<b>Expected Test Results</b>	The TOE should perform an SSH rekey after the configured data limit has been reached.
<b>Pass/Fail with Explanation</b>	Pass, The TOE sends a successful rekey request after the configured amount of data has been elapsed.
<b>Result</b>	Pass

## 7.10 TLSS

### 7.10.1 FCS\_TLSS\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).</p>
<b>Test Steps</b>	<p>TLS_RSA_WITH_AES_128_CBC_SHA</p> <ul style="list-style-type: none"> <li>• Establish a TLS connection from the VM with the TOE using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite via packet capture.</li> </ul>

	<p>TLS_RSA_WITH_AES_256_CBC_SHA</p> <ul style="list-style-type: none"> <li>• Establish a TLS connection from the VM with the TOE using the TLS_RSA_WITH_AES_256_CBC_SHA ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite via packet capture.</li> </ul> <p>TLS_RSA_WITH_AES_128_CBC_SHA256</p> <ul style="list-style-type: none"> <li>• Establish a TLS connection from the VM with the TOE using the TLS_RSA_WITH_AES_128_CBC_SHA256 ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite via packet capture.</li> </ul> <p>TLS_RSA_WITH_AES_256_CBC_SHA256</p> <ul style="list-style-type: none"> <li>• Establish a TLS connection from the VM with the TOE using the TLS_RSA_WITH_AES_256_CBC_SHA256 ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite via packet capture.</li> </ul> <p>TLS_RSA_WITH_AES_128_GCM_SHA256</p> <ul style="list-style-type: none"> <li>• Establish a TLS connection from the VM with the TOE using the TLS_RSA_WITH_AES_128_GCM_SHA256 ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite via packet capture.</li> </ul> <p>TLS_RSA_WITH_AES_256_GCM_SHA384</p> <ul style="list-style-type: none"> <li>• Establish a TLS connection from the VM with the TOE using the TLS_RSA_WITH_AES_256_GCM_SHA384 ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite.</li> <li>• Verify that the session was established with the chosen ciphersuite via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE logs should show the successful establishment of TLS connection.</li> <li>• Packet captures show the successful establishment of TLS connection with configured ciphersuites.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. TOE successfully negotiates each of the claimed cipher suites. This meets the test requirements.
<b>Result</b>	Pass

### 7.10.2 FCS\_TLSS\_EXT.1.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Attempt a connection using Acumen-tlss tool with a certificate, that does not match the ciphersuite. NULL_WITH_NULL_NULL RSA_WITH_NULL_MD5</li> <li>Verify the connection fails with packet capture</li> <li>Verify with logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>Connection should be rejected when an unsupported ciphersuite or the NULL ciphersuite is used.</li> <li>Packet capture shows handshake failure when using unsupported or NULL ciphersuites.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied a connection to a server using a certificate that doesn't match the cipher suite. This meets the test requirements.
<b>Result</b>	Pass

### 7.10.3 FCS\_TLSS\_EXT.1.1 Test #3a

Item	Data
<b>Test Assurance Activity</b>	Test 3: The evaluator shall perform the following modifications to the traffic: a) Modify a byte in the Client Finished handshake message, and verify that the server rejects the connection and does not send any application data.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Use the Acumen-tlss tool to initiate a connection to the TOE and verify that the connection fails with the modified Client Finished handshake message.</li> <li>Verify the connection fails in PCAP.</li> <li>Verify using device failure Logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>TOE should reject a connection when the byte in client finished handshake message is modified.</li> <li>Packet capture should show connection failure when the Client Finished handshake message is modified.</li> <li>The TOE should generate the appropriate logs for failure.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass, when a byte of the Client Finished is changed during the client hello, the TOE does not accept the connection. This meets the testing requirements.
<b>Result</b>	Pass

### 7.10.4 FCS\_TLSS\_EXT.1.1 Test #3b

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>Test 3: The evaluator shall perform the following modifications to the traffic: (Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.)</p> <p>The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent.</p> <p>The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Initiate a TLS connection to the TOE with the acumen-tls tool as a client.</li> <li>• Verify that no Alert with alert level Fatal (2) messages were sent.</li> <li>• Analyzed the traffic to view the Finished message was sent after the ChangeCipherSpec message.</li> <li>• Verify the unsuccessful connection via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE should accept an appropriately encrypted TLS connection.</li> <li>• Evidence (Packet capture) showing the message is encrypted hence the connection is successful.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass, No Alert with alert level Fatal (2) messages were sent. The Finished message is sent immediately after the server's ChangeCipherSpec message. The Finished message does not contain unencrypted data. This meets the testing requirements</p>
<b>Result</b>	<p>Pass</p>

### 7.10.5 FCS\_TLSS\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.</p>

<b>Test Steps &amp;</b>	<ul style="list-style-type: none"> <li>Run the acumen-tls tool as a client to initiate a connection to the TOE and verify the connections fails for all the non-supported SSL and TLS versions.</li> <li>Verify the packet capture to ensure that the TOE rejected the connection. Verify that the log indicated an error with handshake Failure because of an incorrect TLS protocol version.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>Server should reject a connection when a client requests a connection with the unsupported TLS/SSL versions.</li> <li>TOE logs should show connection failure due to an unknown protocol version.</li> <li>Packet capture should show connection failure due to unsupported protocol version.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully connected with all supported protocol versions and rejected unsupported protocol versions. This meets testing requirements.
<b>Result</b>	Pass

### 7.10.6 FCS\_TLSS\_EXT.1.3 Test #1a

Item	Data
<b>Test Assurance Activity</b>	Test 1: [conditional] If ECDHE ciphersuites are supported: <ol style="list-style-type: none"> <li>The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (through a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.</li> </ol>
<b>Pass/Fail with Explanation</b>	NA, TOE does not support ECDHE ciphers.

### 7.10.7 FCS\_TLSS\_EXT.1.3 Test #1b

Item	Data
<b>Test Assurance Activity</b>	Test 1: [conditional] If ECDHE ciphersuites are supported: <ol style="list-style-type: none"> <li>The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.</li> </ol>
<b>Pass/Fail with Explanation</b>	NA, TOE does not support ECDHE ciphers.

### 7.10.8 FCS\_TLSS\_EXT.1.3 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: [conditional] If DHE ciphersuites are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure

	the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).
<b>Pass/Fail with Explanation</b>	NA, TOE does not support DHE ciphers.

### 7.10.9 FCS\_TLSS\_EXT.1.3 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3: [conditional] If RSA key establishment ciphersuites are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.
<b>Test Steps</b>	<p><b>RSA key Size : 2048 bits</b></p> <ul style="list-style-type: none"> <li>Configure TOE to support 2048 RSA key by uploading a certificate with 2048 RSA Key size</li> <li>Run the acumen-tls tool as a client to initiate a to the TOE and verify the connection successful for Supported RSA key Size.</li> <li>Verify the successful connection via packet capture.</li> </ul> <p><b>RSA key Size : 3072 bits</b></p> <ul style="list-style-type: none"> <li>Configure TOE to support 3072 RSA key by uploading a certificate with 3072 RSA Key size</li> <li>Run the acumen-tls tool as a client to initiate a to the TOE and verify the connection successful for Supported RSA key Size.</li> <li>Verify the successful connection via packet capture.</li> </ul> <p><b>RSA key Size : 4096bits</b></p> <ul style="list-style-type: none"> <li>Configure TOE to support 4096 RSA key by uploading a certificate with 4096 RSA Key size</li> <li>Run the acumen-tls tool as a client to initiate a to the TOE and verify the connection successful for Supported RSA key Size.</li> <li>Verify the successful connection via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>TOE should accept supported RSA key establishment key size connections.</li> <li>Evidence (Packet capture) showing the successful connection with configured key size.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE connects successfully with supported RSA key establishment ciphersuite. This meets testing requirements
<b>Result</b>	Pass

### 7.10.10 FCS\_TLSS\_EXT.1.4 Test #1

Item	Data
------	------



<b>Test Assurance Activity</b>	<p><i>Test Objective: To demonstrate that the TOE will not resume a session for which the client failed to complete the handshake (independent of TOE support for session resumption).</i></p> <p>Test 1 [conditional]: If the TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077, the evaluator shall perform the following test:</p> <ol style="list-style-type: none"> <li>a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket.</li> <li>b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake).</li> <li>c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps: Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID.</li> <li>d) The client completes the TLS handshake and captures the SessionID from the ServerHello.</li> <li>e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session using the SessionID captured in step d).</li> <li>f) The client verifies the TOE (1) implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.</li> </ol> <p>Remark: If multiple contexts are supported for session resumption, the session ID or session ticket may be obtained in one context for resumption in another context. It is possible that one or more contexts may only permit the construction of sessions to be reused in other contexts but not actually permit resumption themselves. For contexts which do not permit resumption, the evaluator is required to verify this behaviour subject to the description provided in the TSS. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.</p> <p><b>TD0569 has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<p>NA, The TOE supports Session resumption based on session IDs and session tickets this test is not applicable.</p>

### 7.10.11 FCS\_TLSS\_EXT.1.4 Test #2a

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 [conditional]: If the TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2), the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <ol style="list-style-type: none"> <li>a) The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID</li> </ol>

	<p>immediately followed by ChangeCipherSpec and Finished messages (as shown in Figure 2 of RFC 4346 or RFC 5246).</p> <p>Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ID may be obtained in one context for resumption in another context. There is no requirement that the session ID be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ID constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.</p> <p><b>TD0569 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the openssl s_client -sess_out and -sess_in options to save and resume a session using session ID respectively.</li> <li>• Verify via packet capture that the Client Hello uses the previously captured session ID, to which the TOE responds with Server Hello containing the same session ID, immediately followed by the ChangeCipherSpec and Finished messages.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE accepts a TLS connection that uses a session ID captured from a previously successful and valid TLS session.</li> <li>• TOE resumes the previous session by responding with a ServerHello message containing the same SessionID.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE resumed a previously successful and valid TLS session when presented with the captured session ID. This meets the testing requirements.
<b>Result</b>	Pass

### 7.10.12 FCS\_TLSS\_EXT.1.4 Test #2b

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 [conditional]: If the TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2), the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <p>b) The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its ChangeCipherSpec message thereby disrupting the handshake. The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.</p> <p>Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ID may be obtained in one context for resumption in another context. There is no requirement that the session ID be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ID constructed in another</p>

	<p>context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.</p> <p><b>TD0569 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the acumen-tlss-test tool to: <ul style="list-style-type: none"> <li>○ Initiate a TLS handshake and disrupt it by generating a fatal alert immediately before the client ChangeCipherSpec message, capturing the session ID in the process; and</li> <li>○ Initiate a new Client Hello using the previously captured session ID.</li> </ul> </li> <li>• Verify via packet capture that the TOE implicitly rejects the session ID by sending a ServerHello containing a different SessionID and completes the handshake.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The server does not resume an invalid session.</li> <li>• The server implicitly rejects the previously captured session ID from an invalid session by sending one of its own.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. The TOE implicitly rejects the previously used session ID for an invalid session and sends a ServerHello containing a different session ID and completes the handshake. This meets the testing requirement</p>
<b>Result</b>	<p>Pass</p>

### 7.10.13 FCS\_TLSS\_EXT.1.4 Test #3a

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3 [conditional]: If the TOE supports session tickets according to RFC5077, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <ol style="list-style-type: none"> <li>a) The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with an abbreviated handshake described in Section 3.1 of RFC 5077 and illustrated with an example in figure 2. Of particular note: if the server successfully verifies the client's ticket, then it may renew the ticket by including a NewSessionTicket handshake message after the ServerHello in the abbreviated handshake (which is shown in figure 2). This is not required, however as further clarified in Section 3.3 of RFC 5077.</li> </ol> <p>Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ticket may be obtained in one context for resumption in another context. There is no requirement that the session ticket be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ticket constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.</p> <p><b>TD0556 and TD0569 has been applied.</b></p>

<b>Pass/Fail with Explanation</b>	NA, The TOE does not support Session resumption based on session tickets this test is not applicable.
-----------------------------------	-------------------------------------------------------------------------------------------------------

### 7.10.14 FCS\_TLSS\_EXT.1.4 Test #3b

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3 [conditional]: If the TOE supports session tickets according to RFC5077, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):</p> <p>b) The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator will then modify the session ticket and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.</p> <p>Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ticket may be obtained in one context for resumption in another context. There is no requirement that the session ticket be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ticket constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.</p> <p><b>TD0569 has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	NA, The TOE does not support Session resumption based on session tickets this test is not applicable.

## 7.11 Firewall

### 7.11.1 FFW\_RUL\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and be directed at a host. The evaluator shall verify using a packet sniffer that none of the generated network traffic is permitted through the firewall during initialization

<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>• Configure a filter to drop traffic from a specific source address.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Send continuous traffic from the chosen source address and verify that it is denied.</li> <li>• Reboot the TOE when ping is in progress.</li> <li>• Verify with logs that traffic from the chosen source address was denied.</li> <li>• Verify with Packet Capture that all traffic from the chosen source address was denied during the reboot.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure a filter to drop traffic from a specific source address.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Send continuous traffic from the chosen source address and verify that it is denied.</li> <li>• Reboot the TOE when ping is in progress.</li> <li>• Verify with logs that traffic from the chosen source address was denied.</li> <li>• Verify with Packet Capture that all traffic from the chosen source address was denied during the reboot.</li> </ul>
<b>Expected Test Results</b>	The TOE denies any traffic being passed through while it is being initialized
<b>Pass/Fail with Explanation</b>	Pass. IPv4 and IPv6 packets that would otherwise be denied by the ruleset are not permitted through the TOE during initialization. This meets the testing requirements
<b>Result</b>	Pass

### 7.11.2 FFW\_RUL\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and be directed at a host. The evaluator shall verify using a packet sniffer that none of the generated network traffic is permitted through the firewall during initialization and is only permitted once initialization is complete.</p> <p>Note: The remaining testing associated with application of the ruleset is addressed in the subsequent test evaluation activities.</p>
<b>Test Steps &amp;</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>• Configure a filter to accept traffic with a specific source address.</li> <li>• Apply the filter to the TOE's interface.</li> </ul>

	<ul style="list-style-type: none"> <li>• Send continuous traffic from the specific source address and verify it is accepted.</li> <li>• Reboot the TOE when ping is in progress.</li> <li>• Verify through the firewall log that traffic from a specific source address is allowed after the reboot.</li> <li>• Verify through packet capture that all traffic is denied when the TOE is performing a reboot, but once the TOE is operational, all traffic from the specific source address is allowed.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure a filter to accept traffic with a specific source address.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Send continuous traffic from the specific source address and verify it is accepted.</li> <li>• Reboot the TOE when ping is in progress.</li> <li>• Verify through the firewall log that traffic from a specific source address is allowed after the reboot.</li> <li>• Verify through packet capture that all traffic is denied when the TOE is performing a reboot, but once the TOE is operational, all traffic from the specific source address is allowed.</li> </ul>
<b>Expected Test Results</b>	The TOE does not allow any traffic that is otherwise permitted through until it is fully initialized and online
<b>Pass/Fail with Explanation</b>	Pass. IPv4 and IPv6 Packets that would otherwise be allowed by the ruleset are not permitted through the TOE during initialization. This meets the testing requirements.
<b>Result</b>	Pass

### 7.11.3 FFW\_RUL\_EXT.1.2/FFW\_RUL\_EXT.1.3/FFW\_RUL\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall use the instructions in the guidance documentation to test that state full packet filter firewall rules can be created that permit, drop, and log packets for each of the following attributes:</p> <ul style="list-style-type: none"> <li>• ICMPv4 <ul style="list-style-type: none"> <li>○ Type</li> <li>○ Code</li> </ul> </li> <li>• ICMPv6 <ul style="list-style-type: none"> <li>○ Type</li> <li>○ Code</li> </ul> </li> <li>• IPv4 <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Transport Layer Protocol</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• IPv6 <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Transport Layer Protocol and where defined by the ST author,</li> <li>○ Extension Header Type, Extension Header Fields</li> </ul> </li> <li>• TCP <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> <li>• UDP <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> </ul> <p>Note that these test activities should be performed in conjunction with those of FFW_RUL_EXT.1.9 where the effectiveness of the rules is tested. The test activities for FFW_RUL_EXT.1.9 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfil the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.</p>
<b>Test Steps</b>	<p><b>IPv4</b></p> <p>Source address</p> <ul style="list-style-type: none"> <li>• Configure a filter to drop and accept traffic with specified IPv4 source addresses.</li> <li>• Apply the IPv4 source address filter.</li> <li>• Generate and send traffic that matches the applied filter.</li> <li>• Verify the IPV4 packets are dropped or accepted according to the filter applied using logs.</li> <li>• Verify the IPV4 packets are dropped or accepted according to the filter applied using Packet Capture.</li> </ul> <p>Destination Address</p> <ul style="list-style-type: none"> <li>• Configure a filter to drop and accept traffic with specified IPv4 destination addresses.</li> <li>• Apply the IPv4 destination address filter.</li> <li>• Generate and send traffic that matches the applied filter.</li> <li>• Verify the IPV4 packets are dropped or accepted according to the filter applied using logs.</li> <li>• Verify the IPV4 packets are dropped or accepted according to the filter applied using Packet Capture.</li> </ul> <p>Transport Layer Protocol</p> <ul style="list-style-type: none"> <li>• Configure a filter to drop and accept traffic with a specified IPv4 transport layer protocol.</li> <li>• Apply the IPv4 protocol filter.</li> <li>• Generate and send traffic that matches the applied filter.</li> </ul>

- Verify the IPV4 protocol packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV4 protocol packets are dropped or accepted according to the filter applied using packet capture.

## **IPv6**

### Source address

- Configure a filter to drop and accept traffic with specified IPv6 source addresses.
- Apply the IPv6 source address filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using Packet Capture.

### Destination Address

- Configure a filter to drop and accept traffic with specified IPv6 destination addresses.
- Apply the IPv6 destination address filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using Packet Capture.

### Transport Layer Protocol

- Configure a filter to drop and accept traffic with a specified IPv6 transport layer protocol.
- Apply the IPv6 protocol filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 protocol packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 protocol packets are dropped or accepted according to the filter applied using Packet Capture.

## **TCP**

### Source Port

- Configure a filter to drop and accept traffic according to specified source ports.
- Apply the source port filter.
- Generate and send traffic that matches the applied filter.
- Verify the TCP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

### Destination Port

- Configure a filter to drop and accept traffic according to specified destination ports.



- Apply the destination port filter.
- Generate and send traffic that matches the applied filter.
- Verify the TCP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

## UDP

### Source Port

- Configure a filter to drop and accept traffic according to specified source ports.
- Apply the source port filter.
- Generate and send traffic that matches the applied filter.
- Verify the UDP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

### Destination Port

- Configure a filter to drop and accept traffic according to specified destination ports.
- Apply the destination port filter.
- Generate and send traffic that matches the applied filter.
- Verify the UDP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

## ICMPv4

### Type

- Configure a filter to accept and drop ICMPV4 packets according to its type.
- Apply the ICMPv4 type filter.
- Generate and send traffic that matches the created filter.
- Verify through logs that the ICMPV4 packets are dropped or accepted according to the rules applied based on type.
- Verify the traffic was sent via Wireshark packet capture.

### Code

- Configure a filter to accept and drop ICMPV4 packets according to its code.
- Apply the ICMPv4 type filter.
- Generate and send traffic that matches the created filter.
- Verify through logs that the ICMPV4 packets are dropped or accepted according to the rules applied based on code.
- Verify the traffic was sent via Wireshark packet capture.

## ICMPv6

	<p>Type</p> <ul style="list-style-type: none"> <li>• Configure a filter to accept and drop ICMPV4 packets according to its type.</li> <li>• Apply the ICMPv6 type filter.</li> <li>• Generate and send traffic that matches the created filter.</li> <li>• Verify through logs that the ICMPV6 packets are dropped or accepted according to the rules applied based on type.</li> <li>• Verify the traffic was sent via Wireshark packet capture.</li> </ul> <p>Code</p> <ul style="list-style-type: none"> <li>• Configure a filter to accept and drop ICMPV4 packets according to its code.</li> <li>• Apply the ICMPv6 type filter.</li> <li>• Generate and send traffic that matches the created filter.</li> <li>• Verify through logs that the ICMPV6 packets are dropped or accepted according to the rules applied based on code.</li> <li>• Verify the traffic was sent via Wireshark packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE can perform all packet filtering for IPv4, IPv6, TCP, UDP, ICMP and ICMPv6 properly with the rules configured by the administrator.
<b>Pass/Fail with Explanation</b>	Pass. For IPV4 and IPvE6, TOE successfully implemented full packet filter firewall rules that permit, drop, and log packets for each of the specified attributes. This meets the testing requirements.
<b>Result</b>	Pass

#### 7.11.4 FFW\_RUL\_EXT.1.2/FFW\_RUL\_EXT.1.3/FFW\_RUL\_EXT.1.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: Repeat the test assurance activity above to ensure that state full traffic filtering rules can be defined for each distinct network interface type supported by the TOE.</p> <p>Note that these test activities should be performed in conjunction with those of FFW_RUL_EXT.1.9 where the effectiveness of the rules is tested. The test activities for FFW_RUL_EXT.1.9 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfil the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.</p>
<b>Pass/Fail with Explanation</b>	Pass. "The TOE performs stateful packet filtering on all packets received from or being sent to the External Network, using the MGMT interface or WAN interface."

### 7.11.5 FFW\_RUL\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 1: The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. While the TCP session is being established, the evaluator shall introduce session establishment packets with incorrect flags to determine that the altered traffic is not accepted as part of the session (i.e., a log event is generated to show the ruleset was applied). After a TCP session is successfully established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports, sequence number, flags) one at a time in order to verify that the altered packets are not accepted as part of the established session.</p>
<b>Test Steps</b>	<p><b>IPV4</b></p> <ul style="list-style-type: none"><li>• Configure the TOE to permit and log TCP traffic.</li><li>• Apply the filter to the TOE's interface.</li><li>• Run the Scapy script for establishing a successful TCP session.</li><li>• While session is being established, send packets with a flag that is not an ACK and verify that they are not accepted as part of current session.</li><li>• Verify ack packet is sent which will establish the original connection.</li><li>• Modify each of the session attributes one at a time in next packets and verify the packet is dropped.</li><li>• Source address<ul style="list-style-type: none"><li>○ Verify through logs that the altered packets are logged by the firewall filter.</li><li>○ Verify through the packet capture that the altered packets are not accepted as part of the established session.</li></ul></li><li>• Destination address<ul style="list-style-type: none"><li>○ Verify through logs that the altered packets are logged by the firewall filter.</li><li>○ Verify through the packet capture that the altered packets are not accepted as part of the established session.</li></ul></li><li>• Source port<ul style="list-style-type: none"><li>○ Verify through logs that the altered packets are logged by the firewall filter.</li><li>○ Verify through the packet capture that the altered packets are not accepted as part of the established session.</li></ul></li><li>• Destination port<ul style="list-style-type: none"><li>○ Verify through logs that the altered packets are logged by the firewall filter.</li><li>○ Verify through the packet capture that the altered packets are not accepted as part of the established session.</li></ul></li><li>• Sequence number<ul style="list-style-type: none"><li>○ Verify through logs that the altered packets are logged by the firewall filter.</li></ul></li></ul>

- Verify through the packet capture that the altered packets are not accepted as part of the established session.
- Flags
  - Verify through logs that the altered packets are logged by the firewall filter.
  - Verify through the packet capture that the altered packets are not accepted as part of the established session.

## IPV6

- Configure the TOE to permit and log TCP traffic.
- Apply the filter to the TOE's interface.
- Run the Scapy script for establishing a successful TCP session.
- While session is being established, send packets with a flag that is not an ACK and verify that they are not accepted as part of current session.
- Verify ack packet is sent which will establish the original connection.
- Modify each of the session attributes one at a time in next packets and verify the packet is dropped.
  - Source address
    - Verify through logs that the altered packets are logged by the firewall filter.
    - Verify through the packet capture that the altered packets are not accepted as part of the established session.
  - Destination address
    - Verify through logs that the altered packets are logged by the firewall filter.
    - Verify through the packet capture that the altered packets are not accepted as part of the established session.
  - Source port
    - Verify through logs that the altered packets are logged by the firewall filter.
    - Verify through the packet capture that the altered packets are not accepted as part of the established session.
  - Destination port
    - Verify through logs that the altered packets are logged by the firewall filter.
    - Verify through the packet capture that the altered packets are not accepted as part of the established session.
  - Sequence number
    - Verify through logs that the altered packets are logged by the firewall filter.
    - Verify through the packet capture that the altered packets are not accepted as part of the established session.
  - Flags
    - Verify through logs that the altered packets are logged by the firewall filter.
    - Verify through the packet capture that the altered packets are not accepted as part of the established session.

<b>Expected Test Results</b>	Part-1 <ul style="list-style-type: none"> <li>• TOE firewall logs shows, packets with invalid flags sent while session is being initialized, are not accepted as part of current session since separate log entry is generated.</li> <li>• Packet capture shows the Invalid flag packets are sent before session is established.</li> </ul> Part-2 <ul style="list-style-type: none"> <li>• TOE firewall logs shows, altered packets are not accepted as part of established session.</li> <li>• Packet capture shows separate packets are sent by changing session defining attributes one at a time.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. IPv4 and IPv6 <ul style="list-style-type: none"> <li>• Packets with invalid flags sent while session is being initialized, are not accepted as part of current session.</li> <li>• Packets with altered session defining parameters are not accepted as part of established session.</li> </ul>
<b>Result</b>	Pass

### 7.11.6 FFW\_RUL\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 2: The evaluator shall terminate the TCP session established per Test 1 as described in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset.</p>
<b>Test Steps</b>	IPV4 <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log TCP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Establish a TCP session then terminate the session.</li> <li>• Send a packet that matches the former TCP session.</li> <li>• Verify that the Firewall logs the TCP packet similar to former session.</li> </ul> IPV6 <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log TCP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Establish a TCP session then terminate the session.</li> <li>• Send a packet that matches the former TCP session.</li> <li>• Verify that the Firewall logs and captures the TCP packet similar to former session.</li> </ul>
<b>Expected Test Results</b>	The packets sent matching the former TCP session are subject to the firewall ruleset when being sent through the TOE.

<b>Pass/Fail with Explanation</b>	Pass. Any IPv4 and IPv6 packet matching the TCP former session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.
<b>Result</b>	Pass

### 7.11.7 FFW\_RUL\_EXT.1.5 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 3: The evaluator shall expire (i.e., reach timeout) the TCP session established per Test 1 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.</p>
<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log TCP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Establish a TCP session and wait for the session to expire.</li> <li>• Send a packet that matches the former TCP session.</li> <li>• Verify that the Firewall logs and captures the TCP packet similar to the former session.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log TCP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Establish a TCP session and wait for the session to expire.</li> <li>• Send a packet that matches the former TCP session.</li> <li>• Verify that the Firewall logs and captures the TCP packet similar to the former session.</li> </ul>
<b>Expected Test Results</b>	The packets matching the former TCP session are subject to the firewall ruleset when being forwarded through the TOE.
<b>Pass/Fail with Explanation</b>	Pass. Any IPv4 and IPv6 TCP packet matching the former expired session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.
<b>Result</b>	Pass

### 7.11.8 FFW\_RUL\_EXT.1.5 Test #4

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 4: The evaluator shall configure the TOE to permit and log UDP traffic. The evaluator shall establish a UDP session. Once a UDP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports) one at a time in order to verify that the altered packets are not accepted as part of the established session..</p>
<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log UDP traffic.</li> <li>• Apply the filter to the TOE’s interface.</li> <li>• Establish a UDP session and send data.</li> <li>• Modify each of the session attributes one at a time: <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination address</li> <li>○ Source port</li> <li>○ Destination port</li> </ul> </li> <li>• Verify the altered packets are logged by the firewall filter.</li> <li>• Verify through the packet capture that the altered packets are not accepted as part of the established session.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log UDP traffic.</li> <li>• Apply the filter to the TOE’s interface.</li> <li>• Establish a UDP session and send data.</li> <li>• Modify each of the session attributes one at a time: <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination address</li> <li>○ Source port</li> <li>○ Destination port</li> </ul> </li> <li>• Verify the altered packets are logged by the firewall filter.</li> <li>• Verify through the packet capture that the altered packets are not accepted as part of the established session.</li> </ul>
<b>Expected Test Results</b>	<p>The TOE rejects UDP traffic that are not part of the established UDP session.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass. For IPv4 and IPv6, the TOE does not accept altered packets (source and destination addresses, source and destination ports) after a UDP session is successfully established. This meets the testing requirements.</p>
<b>Result</b>	<p>Pass</p>

### 7.11.9 FFW\_RUL\_EXT.1.5 Test #5

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 5: The evaluator shall expire (i.e., reach timeout) the UDP session established per Test 4 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.</p>
<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log UDP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Establish a UDP session and wait for the session to expire.</li> <li>• Send a packet that matches the former UDP session.</li> <li>• Verify that the Firewall logs the UDP packet similar to former session.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure the TOE to permit and log UDP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Establish a UDP session and wait for the session to expire.</li> <li>• Send a packet that matches the former UDP session.</li> <li>• Verify that the Firewall logs the UDP packet similar to former session.</li> </ul>
<b>Expected Test Results</b>	The packets sent matching the former UDP session are subject to the firewall ruleset when being sent through the TOE.
<b>Pass/Fail with Explanation</b>	Pass. Any IPV4 and IPv6 UDP packet matching the former expired session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.
<b>Result</b>	Pass

### 7.11.10 FFW\_RUL\_EXT.1.5 Test #6

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 6: If ICMP is selected, the evaluator shall configure the TOE to permit and log ICMP traffic. The evaluator shall establish a session for ICMP as defined in the TSS. Once an ICMP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, other attributes chosen in FFW_RUL_EXT.1.5) one at a time in order to verify that the altered packets are not accepted as part of the established session.</p>



## Test Steps

### IPv4

- Configure the TOE to permit and log ICMP traffic.
- Apply the filter to the TOE's interface.
- For each of the session attributes, verify the altered packets are not accepted as part of the session.
  - Source address
    - Establish ICMP connection.
    - Modify session attribute.
    - Verify the altered packets are logged by the firewall filter.
    - Verify the altered packets are not accepted as part of the established session.
  - Destination address
    - Establish ICMP connection.
    - Modify session attribute.
    - Verify the altered packets are logged by the firewall filter.
    - Verify the altered packets are not accepted as part of the established session.
  - Type
    - Establish ICMP connection.
    - Modify session attribute.
    - Verify the altered packets are logged by the firewall filter.
    - Verify the altered packets are not accepted as part of the established session.
  - Code
    - Establish ICMP connection.
    - Modify session attribute.
    - Verify the altered packets are logged by the firewall filter.
    - Verify the altered packets are not accepted as part of the established session.

### IPv6

- Configure the TOE to permit and log ICMP traffic.
- Apply the filter to the TOE's interface.
- For each of the session attributes, verify the altered packets are not accepted as part of the session.
  - Source address
    - Establish ICMP connection.
    - Modify session attribute.
    - Verify the altered packets are logged by the firewall filter.
    - Verify the altered packets are not accepted as part of the established session.

	<ul style="list-style-type: none"> <li>○ Destination address <ul style="list-style-type: none"> <li>● Establish ICMP connection.</li> <li>● Modify session attribute.</li> <li>● Verify the altered packets are logged by the firewall filter.</li> <li>● Verify the altered packets are not accepted as part of the established session.</li> </ul> </li> <li>○ Type <ul style="list-style-type: none"> <li>● Establish ICMP connection.</li> <li>● Modify session attribute.</li> <li>● Verify the altered packets are logged by the firewall filter.</li> <li>● Verify the altered packets are not accepted as part of the established session.</li> </ul> </li> <li>○ Code <ul style="list-style-type: none"> <li>● Establish ICMP connection.</li> <li>● Modify session attribute.</li> <li>● Verify the altered packets are logged by the firewall filter.</li> <li>● Verify the altered packets are not accepted as part of the established session.</li> </ul> </li> </ul>
<b>Expected Test Results</b>	TOE would not accept altered ICMP packets as a part of the established session.
<b>Pass/Fail with Explanation</b>	Pass. For IPv4 and IPv6, TOE did not accept altered packets as a part of established ICMP session (source and destination addresses, type and code). This meets Testing requirements.
<b>Result</b>	Pass

### 7.11.11 FFWD\_RUL\_EXT.1.5 Test #7

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 7: If applicable, the evaluator shall terminate the ICMP session established per Test 6 as described in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset.</p>
<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>● Configure the TOE to permit and log ICMP traffic.</li> <li>● Apply the filter to the TOE's interface.</li> <li>● Establish an ICMP session and terminate it.</li> <li>● Send a packet that matches the former ICMP session.</li> <li>● Verify that the Firewall logs the ICMP packet similar to former session.</li> </ul>

	<ul style="list-style-type: none"> <li>Verify via packet capture that the ICMP packet is similar to the former session.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>Configure the TOE to permit and log ICMP traffic.</li> <li>Apply the filter to the TOE's interface.</li> <li>Establish an ICMP session and terminate it.</li> <li>Send a packet that matches the former ICMP session.</li> <li>Verify that the Firewall logs the ICMP packet similar to former session.</li> <li>Verify via packet capture that the ICMP packet is similar to the former session.</li> </ul>
<b>Expected Test Results</b>	The ICMP traffic is subject to the ruleset configured when forwarded through the TOE.
<b>Pass/Fail with Explanation</b>	Pass. Any IPv4 and IPv6 packet matching the ICMP former session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements
<b>Result</b>	Pass

#### 7.11.12 FFW\_RUL\_EXT.1.5 Test #8

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 8: The evaluator shall expire (i.e., reach timeout) the ICMP session established per Test 6 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.</p>
<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>Configure the TOE to permit and log ICMP traffic.</li> <li>Apply the filter to the TOE's interface.</li> <li>Establish an ICMP session and wait for the session to expire.</li> <li>Send a packet that matches the former ICMP session.</li> <li>Verify that the Firewall logs the ICMP packet similar to former session.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>Configure the TOE to permit and log ICMP traffic.</li> <li>Apply the filter to the TOE's interface.</li> <li>Establish an ICMP session and wait for the session to expire.</li> <li>Send a packet that matches the former ICMP session.</li> </ul>

	<ul style="list-style-type: none"> <li>Verify that the Firewall logs the ICMP packet similar to former session.</li> </ul>
<b>Expected Test Results</b>	The ICMP traffic is subject to the ruleset on the TOE when being forwarded through the TOE.
<b>Pass/Fail with Explanation</b>	Pass. Any IPv4 and IPv6 ICMP packet matching the former expired session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.
<b>Result</b>	Pass

### 7.11.13 FFW\_RUL\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Both IPv4 and IPv6 shall be tested for items a), b), c), d), and e) of the SFR element. Both IPv4 and IPv6 shall be tested for item i) unless the rule definition is specific to IPv4 or IPv6. Note: f), g), and h) are specific to IPv4 or IPv6 and shall be tested accordingly</p> <p>Test 1: The evaluator shall test each of the conditions for automatic packet rejection in turn. In each case, the TOE should be configured to allow all network traffic and the evaluator shall generate a packet or packet fragment that is to be rejected. The evaluator shall use packet captures to ensure that the unallowable packet or packet fragment is not passed through the TOE.</p>
<b>Test Steps</b>	<p>IPV4</p> <p><b>Packets which are invalid fragments.</b></p> <ul style="list-style-type: none"> <li>Create an access-list to log IPv4 packets.</li> <li>Configure the security zone on interface to drop invalid fragments.</li> <li>Send packets which are invalid fragments.</li> <li>Verify through logs that the traffic is rejected.</li> <li>Verify through Packet Capture that the traffic is rejected.</li> </ul> <p><b>Fragments that cannot be completely re-assembled.</b></p> <ul style="list-style-type: none"> <li>Create an access-list to log IPv4 packets.</li> <li>Configure the security zone on interface to drop invalid fragments that cannot be re-assembled.</li> <li>Send fragments that cannot be re-assembled.</li> <li>Verify through logs that the traffic is rejected.</li> <li>Verify through Packet Capture that the traffic is rejected.</li> </ul> <p><b>Packets where the source address is defined as being on a broadcast network.</b></p> <ul style="list-style-type: none"> <li>Create an access-list to log IPv4 packets.</li> <li>Configure the security zone on interface to drop the broadcast packets.</li> <li>Send traffic where the source address is defined as being on a broadcast network.</li> </ul>

- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

**Packets where the source address is defined as being on a multicast network.**

- Create an access-list to log IPv4 packets.
- Configure the security zone on interface to drop the packets with multicast source address.
- Send traffic where the source address is defined as being on a multicast network.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

**Packets where the source address is defined as being a loopback address.**

- Create an access-list to log IPv4 packets.
- Configure the security zone on interface to drop packets with loopback source address.
- Send traffic where the source address is defined as being on a loopback address.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

**Packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4)**

- Create an access-list to log IPv4 packets.
- Configure the security zone on interface to drop packets.
- Send traffic with source address matching unspecified address and reserved for further use.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

**Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.**

- Create an access-list to log IPv4 packets.
- Configure the security zone on interface to drop packet with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.
- Send traffic with IP options: Loose Source Routing, Strict Source Routing, or Record Route.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

- Other packets defined in FFW\_RUL\_EXT.1.6- No other rules defined.

IPV6:

#### **Packets which are invalid fragments.**

- Create an access-list to log IPv6 packets.
- Configure the security zone on interface to drop invalid fragments.
- Send packets which are invalid fragments.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

#### **Fragments that cannot be completely re-assembled.**

- Create an access-list to log IPv6 packets.
- Configure the security zone on interface to drop invalid fragments that cannot be re-assembled.
- Send fragments that cannot be re-assembled.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

#### **Packets where the source address is defined as being on a broadcast network.**

- Create an access-list to log IPv6 packets.
- Configure the security zone on interface to drop broadcast packets.
- Send traffic where the source address is defined as being on a broadcast network.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

#### **Packets where the source address is defined as being on a multicast network.**

- Create an access-list to log IPv6 packets.
- Configure the security zone on interface to drop packets with multicast source address.
- Send traffic where the source address is defined as being on a multicast network.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

#### **Packets where the source address is defined as being a loopback address.**

- Create an access-list to log IPv6 packets.
- Configure the security zone on interface to drop packets with loopback source address.
- Send traffic where the source address is defined as being on a loopback address.
- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

	<p><b>Packets where the source or destination address of the network packet is defined as being unspecified or an address “reserved for future use”</b></p> <ul style="list-style-type: none"> <li>○ Create an access-list to log IPv6 packets.</li> <li>○ Configure the security zone on interface to drop packets.</li> <li>○ Send traffic with source address matching unspecified address and reserved for further use.</li> <li>○ Verify through logs that the traffic is rejected.</li> <li>○ Verify through Packet Capture that the traffic is rejected.</li> </ul>
<b>Expected Test Results</b>	The ruleset on the TOE allows all valid traffic through and rejects any fragmented or invalid packets.
<b>Pass/Fail with Explanation</b>	Pass. For IPv4 and IPv6 each of the conditions ( invalid fragment, unreassembled fragments, broadcast network source address, multicast network source address, loopback address, unspecified or reserved address, and packets with IPv4 options) are rejected and logged automatically.
<b>Result</b>	Pass

#### 7.11.14 FFW\_RUL\_EXT.1.6 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Both IPv4 and IPv6 shall be tested for items a), b), c), d), and e) of the SFR element. Both IPv4 and IPv6 shall be tested for item i) unless the rule definition is specific to IPv4 or IPv6. Note: f), g), and h) are specific to IPv4 or IPv6 and shall be tested accordingly</p> <p>Test 2: For each of the cases above, the evaluator shall use any applicable guidance to enable dropped packet logging or counting. In each case above, the evaluator shall ensure that the rejected packet or packet fragment was recorded (either logged or an appropriate counter incremented).</p>
<b>Pass/Fail with Explanation</b>	Pass. The requirements of this test have been completed as part of testing for FFW_RUL_EXT.1.6 Test #1.
<b>Result</b>	Pass

#### 7.11.15 FFW\_RUL\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 1: The evaluator shall configure the TOE to drop and log network traffic where the source address of the packet matches that of the TOE network interface upon which the traffic was received.</p>

	The evaluator shall generate suitable network traffic to match the configured rule and verify that the traffic is dropped, and a log message generated.
<b>Test Steps</b>	<p>IPV4</p> <ul style="list-style-type: none"> <li>• Configure a filter to log and drop traffic when the source address of the packet matches the address of the network interface.</li> <li>• Apply the filter on TOE interface.</li> <li>• Generate and send traffic that matches the created filter.</li> <li>• Verify through the firewall filter that the traffic was denied.</li> <li>• Verify through a packet capture that the traffic was denied.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure a filter to log and drop traffic when the source address of the packet matches the address of the network interface.</li> <li>• Apply the filter on TOE interface.</li> <li>• Generate and send traffic that matches the created filter.</li> <li>• Verify through the firewall filter that the traffic was denied.</li> <li>• Verify through a packet capture that the traffic was denied.</li> </ul>
<b>Expected Test Results</b>	The TOE rejects network traffic where the source address of the packet matches the TOE interface upon where traffic was received.
<b>Pass/Fail with Explanation</b>	Pass. The TOE dropped and logged the IPv4 and IPv6 packets where the source address of the packet matches that of the TOE network interface upon which the traffic was received. This meets testing requirements
<b>Result</b>	Pass

### 7.11.16 FFW\_RUL\_EXT.1.7 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 2: The evaluator shall configure the TOE to drop and log network traffic where the source IP address of the packet fails to match the network reachability information of the interface to which it is targeted, e.g. if the TOE believes that network 192.168.1.0/24 is reachable through interface 2, network traffic with a source address from the 192.168.1.0/24 network should be generated and sent to an interface other than interface 2. The evaluator shall verify that the network traffic is dropped, and a log message generated.</p>
<b>Test Steps</b>	<p>IPv4</p> <ul style="list-style-type: none"> <li>• Configure TOE interface to drop and log network traffic when the source IP address of the packet does not match the interface it was received on.</li> </ul>



	<ul style="list-style-type: none"> <li>• Verify Firewall doesn't have correct route for source IP address.</li> <li>• Initiate traffic with Ping.</li> <li>• Verify through the logs and a packet capture that the traffic is dropped.</li> <li>• Verify the packets are dropped via Packet Capture.</li> </ul> <p>IPv6</p> <ul style="list-style-type: none"> <li>• Configure TOE interface to drop and log network traffic when the source IP address of the packet does not match the interface it was received on.</li> <li>• Verify Firewall doesn't have correct route for source IP address.</li> <li>• Initiate traffic with Ping.</li> <li>• Verify through the logs and a packet capture that the traffic is dropped.</li> <li>• Verify the packets are dropped via Packet Capture.</li> </ul>
<b>Expected Test Results</b>	Log Message and Packet capture shows that TOE drops the packet when source IP address of the packet fails to match the network reachability information of the interface to which it is targeted.
<b>Pass/Fail with Explanation</b>	Pass. TOE dropped and logged the IPv4 and IPv6 packets where the source IP address of the packet fails to match the network reachability information of the interface to which it is targeted. This meets the testing requirements.
<b>Result</b>	Pass

7.11.17 FFW\_RUL\_EXT.1.8 Test #1

Item	Data
<p><b>Test Assurance Activity</b></p>	<p>Test 1: If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the evaluator shall try to configure two conflicting rules and verify that the TOE rejects the conflicting rule(s). It is important to verify that the mechanism is implemented in the TOE but not in the non-TOE environment. If the TOE does not implement a mechanism that ensures that no conflicting rules can be configured, the evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.</p> <p><b>TD0545 has been applied.</b></p>
<p><b>Test Steps</b></p>	<p>IPV4:</p> <ul style="list-style-type: none"> <li>• Configure a filter to allow and drop packets that have the same destination-address with the allow rule being first.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send traffic to configured destination address in filter.</li> <li>• Verify through the firewall log that traffic is allowed.</li> <li>• Verify allowed traffic via packet capture.</li> <li>• Configure a filter to drop and allow packets that have the same destination-address with the drop rule being first.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send traffic to configured destination address in filter.</li> <li>• Verify through the firewall log that traffic is discarded.</li> <li>• Verify via packet capture discarded traffic.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure a filter to allow and drop packets that have the same destination-address with the allow rule being first.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send traffic to configured destination address in filter.</li> <li>• Verify through the firewall log that traffic is allowed.</li> <li>• Verify allowed traffic via packet capture.</li> <li>• Configure a filter to drop and allow packets that have the same destination-address with the drop rule being first.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send traffic to configured destination address in filter.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify through the firewall log that traffic is discarded.</li> <li>• Verify via packet capture discarded traffic.</li> </ul>
<b>Expected Test Results</b>	The TOE rejects the configuration of two conflicted rules as well as enforcing the rule in the order in which they are configured where the first rule is enforced before any following rules.
<b>Pass/Fail with Explanation</b>	Pass. For IPV4 and IPv6, TOE enforced the first rule in the firewall filter. This meets the testing requirement.
<b>Result</b>	Pass

### 7.11.18 FFW\_RUL\_EXT.1.8 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
<b>Test Steps</b>	<p>IPV4:</p> <ul style="list-style-type: none"> <li>• Configure the firewall rule order to allow packets to a specific destination-address and deny packets to its network segment.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send traffic to configured specific destination and network segment addresses.</li> <li>• Verify through the firewall logs that only traffic to specific destination address are allowed and remaining addresses to network segment are discarded.</li> <li>• Verify the rules applied through Packet Capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the firewall rule order to deny packets to a network segment and allow packets to a specific destination-address of the network segment.</li> <li>• Apply the filter to the TOE Interface</li> <li>• Send traffic to configured specific destination and network segment addresses.</li> <li>• Verify through the firewall logs that all traffic is dropped.</li> <li>• Verify the rules applied through Packet Capture.</li> </ul> <p>IPV6</p> <ul style="list-style-type: none"> <li>• Configure the firewall rule order to allow packets to a specific destination-address and deny packets to its network segment.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send traffic to configured specific destination and network segment addresses.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify through the firewall logs that only traffic to specific destination address are allowed and remaining addresses to network segment are discarded.</li> <li>• Verify the rules applied through Packet Capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the firewall rule order to deny packets to a network segment and allow packets to a specific destination-address of the network segment.</li> <li>• Apply the filter to the TOE Interface</li> <li>• Send traffic to configured specific destination and network segment addresses.</li> <li>• Verify through the firewall logs that all traffic is dropped.</li> <li>• Verify the rules applied through Packet Capture.</li> </ul>
<b>Expected Test Results</b>	The TOE enforces the rules in the order in which they are configured (first rule is enforced, second is after, etc.)
<b>Pass/Fail with Explanation</b>	Pass. For IPv4 and IPv6, TOE enforced the first rule in the firewall filter. This meets the testing requirement
<b>Result</b>	Pass

#### 7.11.19 FFW\_RUL\_EXT.1.9 Test #1

Item	Data
<b>Test Assurance Activity</b>	For each attribute in FFW_RUL_EXT.1.2, the evaluator shall construct a test to demonstrate that the TOE can correctly compare the attribute from the packet header to the ruleset, and shall demonstrate both the permit and deny for each case. It shall also be verified that a packet is dropped if no matching rule can be identified for the packet. The evaluator shall check the log in each case to confirm that the relevant rule was applied. The evaluator shall record a packet capture for each test to demonstrate the correct TOE behaviour.
<b>Pass/Fail with Explanation</b>	Pass. This test has been completed as part of FFW_RUL_EXT.1.2.
<b>Result</b>	Pass

#### 7.11.20 FFW\_RUL\_EXT.1.10 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 1: The evaluator shall define a TCP half-open connection limit on the TOE. The evaluator shall generate TCP SYN requests to pass through the TOE to the target system using a</p>

	randomised source IP address and common destination IP address. The number of SYN requests should exceed the TCP half-open threshold defined on the TOE. TCP SYN-ACK messages should not be acknowledged. The evaluator shall verify through packet capture that once the defined TCP half-open threshold has been reached, subsequent TCP SYN packets are not transmitted to the target system. The evaluator shall verify that when the configured threshold is reached that, depending upon the selection, either a log entry is generated or a counter is incremented.
<b>Test Steps</b>	<p>IPV4:</p> <ul style="list-style-type: none"> <li>• Configure the TOE to limit the amount of half-open TCP connections.</li> <li>• Apply the configuration to the TOE's interface.</li> <li>• Send continuous traffic to the TOE.</li> <li>• Verify that when the configured threshold is reached a counter is incremented.</li> <li>• Verify with packet capture.</li> </ul> <p>IPV6:</p> <ul style="list-style-type: none"> <li>• Configure the TOE to limit the amount of half-open TCP connections.</li> <li>• Apply the configuration to the TOE's interface.</li> <li>• Send continuous traffic to the TOE.</li> <li>• Verify that when the configured threshold is reached a counter is incremented.</li> <li>• Verify with packet capture.</li> </ul>
<b>Expected Test Results</b>	The TOE enforces the TCP half-open rules as configured by the administrator.
<b>Pass/Fail with Explanation</b>	Pass. For IPv4 and IPv6, randomized source TCP SYN packets are not transmitted by the TOE. When the configured threshold is reached, a counter is incremented by the TOE. This meets the testing requirements.
<b>Result</b>	Pass

## 7.12 Update

### 7.12.1 FPT\_TST\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>It is expected that at least the following tests are performed:</p> <ul style="list-style-type: none"> <li>a) Verification of the integrity of the firmware and executable software of the TOE</li> <li>b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.</li> </ul> <p>The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this.</p> <p>For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.</p>

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator verifies the integrity of the TOE image with the boot image verification.</li> <li>• Reboot the TOE.</li> <li>• Verify that cryptographic functions, integrity of the firmware and self-tests were performed correctly.</li> <li>• The evaluator displays log evidence of the process.</li> </ul> <p>Note: - All software on the TOE is in the firmware.</p>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should execute all claimed self-tests during bootup.</li> <li>• Evidence (screenshot or CLI output) showing successful self-tests.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully verifies the integrity of firmware and self-tests were performed correctly.
<b>Result</b>	Pass

### 7.12.2 FPT\_TST\_EXT.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall verify that the self test mechanism includes a certificate validation according to FIA_X509_EXT.1 and a check for the Code Signing purpose in the extendedKeyUsage. It is not necessary to verify the revocation status of X.509 certificates during power-up.
<b>Pass/Fail with Explanation</b>	N/A, AS TOE Does not support a self-test mechanism including certificate validation.

### 7.12.3 FPT\_TUD\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE.</p> <p>(For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.)</p> <p>After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator displays the current version of software.</li> <li>• The evaluator uploads a new software image to the TOE.</li> <li>• The evaluator verifies the update file.</li> <li>• The evaluator configures the TOE to boot using the new image.</li> <li>• The evaluator reloads the TOE.</li> <li>• The evaluator displays the new version of software that is loaded.</li> <li>• The evaluator displays log evidence of the image being successfully loaded.</li> </ul>

<b>Expected Test Results</b>	The TOE should successfully allow the new image to be loaded to the TOE.
<b>Pass/Fail with Explanation</b>	Pass, The TOE allows the new image to be successfully loaded.
<b>Result</b>	Pass

#### 7.12.4 FPT\_TUD\_EXT.1 Test #2 (a)

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted).</p> <p>The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>1) A modified version (e.g. using a hex editor) of a legitimately signed update</p> <p>If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator confirms the current version of the TOE.</li> <li>• The evaluator displays the digital signature of the currently loaded image.</li> <li>• The evaluator displays the digital signature of the modified image.</li> <li>• The evaluator attempts to load the modified image to the TOE.</li> <li>• The evaluator displays evidence of the image getting rejected on reboot.</li> <li>• The evaluator attempts to load the previous working image.</li> </ul>
<b>Expected Test Results</b>	The TOE should successfully deny the loading of the modified image.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully rejects loading of the modified image allowing the evaluator to revert back to the previous working image.
<b>Result</b>	Pass

#### 7.12.5 FPT\_TUD\_EXT.1 Test #2 (b)

Item	Data
<b>Test Assurance Activity</b>	[conditional]: If <b>the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE</b> the following test shall be performed (otherwise the test shall be omitted).

	<p>The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>2) An image that has not been signed</p> <p>If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator confirms the current version of the TOE.</li> <li>• The evaluator displays the digital signature of the currently loaded image.</li> <li>• The evaluator displays the digital signature of the modified image.</li> <li>• The evaluator attempts to load the modified image to the TOE.</li> <li>• The evaluator displays evidence of the image getting rejected on reboot.</li> <li>• The evaluator attempts to load the previous working image.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow the modified image to be loaded by the evaluator.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully rejects loading of the modified image allowing the evaluator to revert back to the previous working image.
<b>Result</b>	Pass

### 7.12.6 FPT\_TUD\_EXT.1 Test #2 (c)

Item	Data
<b>Test Assurance Activity</b>	<p>[conditional]: If <b>the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE</b> the following test shall be performed (otherwise the test shall be omitted).</p> <p>The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature)</p> <p>If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE</p>



	has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator confirms the current version of the TOE.</li> <li>• The evaluator displays the digital signature of the currently loaded image.</li> <li>• The evaluator displays the digital signature of the modified image.</li> <li>• The evaluator attempts to load the modified image to the TOE.</li> <li>• The evaluator displays evidence of the image getting rejected on reboot.</li> <li>• The evaluator attempts to load the previous working image.</li> </ul>
<b>Expected Test Results</b>	The TOE should not allow the modified image to be loaded by the evaluator.
<b>Pass/Fail with Explanation</b>	Pass, The TOE successfully rejects loading of the modified image allowing the evaluator to revert back to the previous working image.
<b>Result</b>	Pass

### 7.12.7 FPT\_TUD\_EXT.1 Test #3 (a)

Item	Data
<b>Test Assurance Activity</b>	<p>[conditional]: If <b>the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE</b>, the following test shall be performed (otherwise the test shall be omitted).</p> <p>If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces an illegitimate update such that the hash of the update does not match the published hash. The evaluator provides the published hash value to the TOE and calculates the hash of the update either on the TOE itself (if that functionality is provided by the TOE), or else outside the TOE. The evaluator confirms that the hash values are different, and attempts to install the update on the TOE, verifying that this fails because of the difference in hash values (and that the failure is logged). Depending on the implementation of the TOE, the TOE might not allow the Security Administrator to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE</p> <p>If the TOE allows delayed activation of updates, the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.</p>

Pass/Fail with Explanation	N/A , TOE does not support verification of Hash values.
----------------------------	---------------------------------------------------------

### 7.12.8 FPT\_TUD\_EXT.1 Test #3 (b)

Item	Data
Test Assurance Activity	<p>[conditional]: If <b>the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE</b>, the following test shall be performed (otherwise the test shall be omitted).</p> <p>If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator uses a legitimate update and tries to perform verification of the hash value without providing the published hash value to the TOE. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the verification of the hash value without providing a hash value to the TOE, e.g. if the hash value needs to be handed over to the TOE as a parameter in a command line message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the mechanism that prevents the execution of this check shall be tested accordingly, e.g. that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE</p> <p>If the TOE allows delayed activation of updates, the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.</p>
Pass/Fail with Explanation	N/A , TOE does not support verification of Hash values.

## 8 CAVP Algorithm Certificate Details

The TOE uses OpenSSL 3.0.8 and the associated algorithms are presented in the table below. The CAVP certificate is A4573.

**Table 1 – CAVP Algorithm Certificate References**

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	KlasOS Keel	RSA KeyGen	#A4573
	ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	KlasOS Keel	ECDSA KeyGen	#A4573
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526, RFC 7919].	KlasOS Keel	Safe-Primes key generation Safe-Primes Key Verification	#A4573
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"	KlasOS Keel	None: CCTL tested as per the PP/SD Evaluation Activities	Tested with known-good implementation
	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	KlasOS Keel	KAS-ECC-SSC	#A4573
	FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].	KlasOS Keel	KAS-FFC-SSC	#A4573
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR, and GCM] mode and cryptographic key sizes [128 bits, 256 bits]	KlasOS Keel	AES-CBC 128 bits, 256 bits AES-GCM 128 bits, 256 bits	#A4573

			AES-CTR 128 bits, 256 bits	
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	KlasOS Keel	RSA-SigGen RSA-SigVer 2048, 3072 and 4096	#A4573
	For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4	KlasOS Keel	ECDSA-SigGen ECDSA-SigVer P-256, P-384, P-521	#A4573
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits	KlasOS Keel	SHA-1 SHA2-256 SHA2-384 SHA2-512	#A4573
FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160, 256, 384, and 512 bits] and message digest sizes [160, 256, 384, 512] bits	KlasOS Keel	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	#A4573
FCS_RBG_EXT.1	CTR_DRBG (AES-256)	KlasOS Keel	Counter DRBG AES 256	#A4573

## 9 Conclusion

The testing shows that all test cases required for conformance have passed testing.

**End of Document**