



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12

# Security Target for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000, version JE-1.10-H



Author: RICOH COMPANY, LTD.  
Date: 2021-11-18  
Version: 1.1

13	<b>Table of Contents</b>		
14	1	ST Introduction (ASE_INT).....	7
15	1.1	ST Reference.....	7
16	1.2	TOE Reference.....	7
17	1.3	TOE Variants.....	19
18	1.3.1	Print speed variants.....	19
19	1.3.2	Regional variants.....	19
20	1.3.3	Branding variants.....	19
21	1.4	Evaluated and tested configurations.....	20
22	1.4.1	Required TOE components.....	20
23	1.4.2	Optional TOE components.....	20
24	1.4.3	Required non-TOE components.....	20
25	1.4.4	Optional non-TOE components.....	20
26	1.5	TOE Overview.....	21
27	1.5.1	TOE Type.....	21
28	1.5.2	TOE Usage.....	21
29	1.5.3	Major Security Features of TOE.....	22
30	1.6	TOE Description.....	23
31	1.6.1	Physical Boundary of TOE.....	23
32	1.6.2	Hardware components.....	24
33	1.6.3	Logical Boundary of the TOE.....	26
34	1.6.4	Basic Functions.....	26
35	1.6.5	Security Functions.....	27
36	1.6.6	Functions supported but not evaluated.....	28
37	1.6.7	Guidance Documents.....	29
38	2	ST Conformance Claims (ASE_CCL).....	30
39	2.1	Common Criteria (CC) conformance claims.....	30
40	2.2	Protection Profile (PP) conformance claims.....	30
41	2.3	Conformance Claim Rationale.....	31
42	2.3.2	Consistency Claim with Security Problems and Security Objectives in PP.....	31
43	2.3.3	Consistency Claim with Security Requirements in PP.....	31
44	3	Security Problem Definitions (ASE_SPD).....	32
45	3.1	Users.....	32
46	3.2	Assets.....	32
47	3.2.1	User Data.....	32
48	3.2.2	TSF Data.....	33
49	3.3	Threat definitions.....	33
50	3.4	Organizational Security Policies.....	34
51	3.5	Assumptions.....	34
52	4	Security Objectives (ASE_OBJ).....	35
53	4.1	Security Objectives for the TOE.....	35
54	4.2	Security Objectives for the Operational Environment.....	35
55	4.3	Security Objectives rationale.....	36
56	5	Extended Component Definitions (ASE_ECD).....	38

57	6	Security Functional Requirements (ASE_REQ) .....	39
58	6.1	Notational conventions .....	39
59	6.2	Class FAU: Security Audit .....	39
60	6.2.1	FAU_GEN.1 Audit data generation .....	39
61	6.2.2	FAU_GEN.2 User identity association .....	40
62	6.2.3	FAU_SAR.1 Audit review .....	41
63	6.2.4	FAU_SAR.2 Restricted audit review.....	41
64	6.2.5	FAU_STG.1 Protected audit trail storage .....	42
65	6.2.6	FAU_STG_EXT.1 Extended: External Audit Trail Storage .....	42
66	6.2.7	FAU_STG.4 Prevention of audit data loss.....	43
67	6.3	Class FCO: Communication.....	44
68	6.4	Class FCS: Cryptographic Support .....	44
69	6.4.1	FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) .....	44
70	6.4.2	FCS_CKM.1(b)[DAR] Cryptographic key generation (Symmetric Keys) [Data At Rest] .....	45
71	6.4.3	FCS_CKM.1(b)[DIM] Cryptographic key generation (Symmetric Keys) [Data In Motion].....	46
72	6.4.4	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction.....	46
73	6.4.5	FCS_CKM.4 Cryptographic key destruction .....	47
74	6.4.6	FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption) .....	50
75	6.4.7	FCS_COP.1(b) Cryptographic Operation (for signature generation/verification).....	50
76	6.4.8	FCS_COP.1(c)[L1] Cryptographic operation (Hash Algorithm) .....	51
77	6.4.9	FCS_COP.1(c) [L2] Cryptographic operation (Hash Algorithm).....	53
78	6.4.10	FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).....	54
79	6.4.11	FCS_COP.1(f) Cryptographic operation (Key Encryption).....	57
80	6.4.12	FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) .....	57
81	6.4.13	FCS_HTTPS_EXT.1 Extended: HTTPS selected .....	58
82	6.4.14	FCS_IPSEC_EXT.1 Extended: IPsec selected .....	58
83	6.4.15	FCS_KYC_EXT.1 Extended: Key Chaining .....	66
84	6.4.16	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation) .....	67
85	6.4.17	FCS_TLS_EXT.1 Extended: TLS selected.....	69
86	6.5	Class FDP: User Data Protection.....	71
87	6.5.1	FDP_ACC.1 Subset access control .....	74
88	6.5.2	FDP_ACF.1 Security attribute based access control .....	75
89	6.5.3	FDP_DSK_EXT.1 Extended: Protection of Data on Disk.....	75
90	6.5.4	FDP_FXS_EXT.1 Extended: Fax separation .....	77
91	6.5.5	FDP_RIP.1(a) Subset residual information protection.....	78
92	6.6	Class FIA: Identification and Authentication .....	79
93	6.6.1	FIA_AFL.1 Authentication failure handling.....	79
94	6.6.2	FIA_ATD.1 User attribute definition .....	80
95	6.6.3	FIA_PMG_EXT.1 Extended: Password Management.....	80
96	6.6.4	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition.....	81
97	6.6.5	FIA_UAU.1 Timing of authentication.....	83
98	6.6.6	FIA_UAU.7 Protected authentication feedback .....	84
99	6.6.7	FIA_UID.1 Timing of identification .....	85
100	6.6.8	FIA_USB.1 User-subject binding.....	85

101	6.7	Class FMT: Security Management .....	86
102	6.7.1	FMT_MOF.1 Management of security functions behavior .....	86
103	6.7.2	FMT_MSA.1 Management of security attributes .....	87
104	6.7.3	FMT_MSA.3 Static attribute initialization .....	88
105	6.7.4	FMT_MTD.1 Management of TSF data .....	88
106	6.7.5	FMT_SMF.1 Specification of Management Functions .....	108
107	6.7.6	FMT_SMR.1 Security roles .....	110
108	6.8	Class FPR: Privacy .....	110
109	6.9	Class FPT: Protection of the TSF .....	110
110	6.9.1	FPT_KYP_EXT.1 Extended: Protection of Key and Key Material .....	110
111	6.9.2	FPT_SKP_EXT.1 Extended: Protection of TSF Data .....	111
112	6.9.3	FPT_STM.1 Reliable time stamps .....	111
113	6.9.4	FPT_TST_EXT.1 Extended: TSF testing .....	112
114	6.9.5	FPT_TUD_EXT.1 Extended: Trusted Update .....	112
115	6.10	Class FRU: Resource Utilization .....	113
116	6.11	Class FTA: TOE Access .....	114
117	6.11.1	FTA_SSL.3 TSF-initiated termination .....	114
118	6.12	Class FTP: Trusted Paths/Channels .....	114
119	6.12.1	FTP_ITC.1[IPsec] Inter-TSF trusted channel .....	114
120	6.12.2	FTP_TRP.1(a) Trusted path (for Administrators) .....	116
121	6.12.3	FTP_TRP.1(b) Trusted path (for Non-administrators) .....	117
122	7	Security Assurance Requirements (APE_REQ) .....	119
123	7.1	Class ASE: Security Target evaluation .....	119
124	7.2	Class ADV: Development .....	119
125	7.2.1	ADV_FSP.1 Basic functional specification .....	120
126	7.3	Class AGD: Guidance Documents .....	121
127	7.3.1	AGD_OPE.1 Operational user guidance .....	121
128	7.3.2	AGD_PRE.1 Preparative procedures .....	122
129	7.4	Class ALC: Life-cycle Support .....	123
130	7.4.1	ALC_CMC.1 Labelling of the TOE .....	123
131	7.4.2	ALC_CMS.1 TOE CM coverage .....	123
132	7.5	Class ATE: Tests .....	124
133	7.5.1	ATE_IND.1 Independent testing - Conformance .....	124
134	7.6	Class AVA: Vulnerability Assessment .....	125
135	7.7	Security Assurance Requirements rationale .....	126
136	8	TOE Summary Specification (ASE_TSS) .....	127
137	8.1	Identification and Authentication, Use-of-Feature Authorization (TSF_FIA) .....	127
138	8.1.1	FIA_UAU.1 and FIA_UID.1 .....	127
139	8.1.2	FIA_PMG_EXT.1 .....	127
140	8.1.3	FIA_UAU.7 .....	127
141	8.1.4	FIA_AFL.1 .....	127
142	8.1.5	FIA_USB.1 and FIA_ATD.1 .....	128
143	8.1.6	FTA_SSL.3 .....	128
144	8.2	Access Control (TSF_FDP) .....	128

145	8.2.1	FDP_ACC.1 and FDP_ACF.1 .....	128
146	8.3	Stored Data Encryption (TSF_FCS).....	129
147	8.3.1	FCS_KYC_EXT.1, FPT_KYP_EXT.1, and FCS_COP.1(f) .....	130
148	8.3.2	FCS_CKM.1(b)[DIM], FCS_CKM.1(b)[DAR], and FCS_RBG_EXT.1 .....	130
149	8.3.3	FCS_CKM.4 and FCS_CKM_EXT.4 .....	130
150	8.3.4	FDP_DSK_EXT.1 and FCS_COP.1(d) .....	130
151	8.4	Trusted Communications (TSF_FTP).....	131
152	8.4.1	FTP_TRP.1 (a), FTP_TRP.1 (b), FCS_HTTPS_EXT.1, and FCS_TLS_EXT.1.....	131
153	8.4.2	FCS_CKM.1 (a), FCS_RBG_EXT.1, FCS_COP.1 (a), FCS_COP.1(b)[DIM], FCS_COP.1(c) , and	
154		FCS_COP.1(g).....	131
155	8.4.3	FPT_SKP_EXT.1, FCS_CKM.4 and FCS_CKM_EXT.4.....	131
156	8.4.4	FCS_ITC.1[IPsec], FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, and FCS_COP.1(g) .....	132
157	8.5	Administrative Roles (TSF_FMT) .....	133
158	8.5.1	FMT_SMR.1 .....	133
159	8.5.2	FMT_SMF.1, FMT_MOF.1, and FMT_MTD.1.....	133
160	8.5.3	FMT_MSA.1 and FMT_MSA.3.....	133
161	8.6	Audit Function (TSF_FAU) .....	134
162	8.6.1	FAU_GEN.1 and FAU_GEN.2.....	134
163	8.6.2	FAU_STG.1, FAU_STG_EXT.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2.....	135
164	8.6.3	FPT_STM.1.....	135
165	8.7	Trusted Operation (TSF_FPT) .....	135
166	8.7.1	FPT_TST_EXT.1, FCS_COP.1(b), FCS_COP.1(c)[L1], and FCS_COP.1(c)[L2] .....	135
167	8.7.2	FPT_TUD_EXT.1, FCS_COP.1(b), FCS_COP.1(c)[L1], and FCS_COP.1(c)[L2] .....	136
168	8.8	PSTN Fax-Line Separation (TSF_FXS) .....	137
169	8.8.1	FDP_FXS_EXT.1.....	137
170	8.9	Image Overwrite.....	137
171	8.9.1	FDP_RIP.1(a).....	137
172	A	Terminology .....	139
173	A.1	Glossary.....	139
174	A.2	Acronyms.....	142
175			

176 **List of Figures**

177	Figure 1	Example of TOE Environment.....	22
178	Figure 2	Hardware Configuration of the TOE.....	24
179	Figure 3	Logical Boundary of the TOE .....	26
180			

181 **List of Tables**

182	Table 1	Required TOE components.....	20
183	Table 2	Optional TOE components .....	20
184	Table 3	Required non-TOE components .....	20
185	Table 4	Optional non-TOE components.....	21

186	Table 5 Protection Profile claims .....	30
187	Table 6 User categories.....	32
188	Table 7 Asset categories.....	32
189	Table 8 User Data types .....	32
190	Table 9 Document and Job Attributes.....	32
191	Table 10 TSF Data types .....	33
192	Table 11 Data in D.TSF.PROT.....	33
193	Table 12 Data in D.TSF.CONF .....	33
194	Table 13 Threats.....	34
195	Table 14 Organizational Security Policies.....	34
196	Table 15 Assumptions .....	34
197	Table 16 Security Objectives for the TOE.....	35
198	Table 17 Security Objectives for the Operational Environment .....	35
199	Table 18 Security Objectives rationale.....	37
200	Table 19 Auditable Events.....	40
201	Table 20 D.USER.DOC Access Control SFP.....	72
202	Table 21 D.USER.JOB Access Control SFP.....	73
203	Table 22 Authentication Events .....	79
204	Table 23 List of Actions for Authentication Failure .....	79
205	Table 24 Rules for Initial Association of Attributes.....	85
206	Table 25 User Roles for Security Attributes .....	87
207	Table 26 List of Administrator-only TSF Data, Operations, and Roles.....	107
208	Table 27 List of Additional TSF Data, Operations, and Roles .....	108
209	Table 28 TOE Security Assurance Requirements.....	119
210	Table 29 Stored Documents Access Control Rules for Normal Users .....	129
211	Table 30 Keychain encryption .....	130
212	Table 31 Random Number Sources.....	130
213	Table 32 Storage encryption cryptographic functions .....	130
214	Table 33 TLS/HTTPS cryptographic functions.....	131
215	Table 34 IPsec cryptographic functions.....	132
216	Table 35 List of Static Initialization for Security Attributes of Document Access Control SFP .....	134
217	Table 36 Roles allowed to override default values .....	134
218	Table 37 List of Audit Events .....	134
219	Table 38 Start-up integrity tests.....	136
220	Table 39 Glossary of Terms .....	141
221	Table 40 Acronyms.....	142
222		

## 223 1 ST Introduction (ASE\_INT)

### 224 1.1 ST Reference

225 The following are the identification information of this ST.

- 226 • Title: Security Target for RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000 version JE-  
227 1.10-H
- 228 • Version: 1.1
- 229 • Date: 2021-11-19
- 230 • Author: RICOH COMPANY, LTD.
- 231 • Keywords: multifunction, hardcopy, MFD, MFP, HCD, printer, copier, scanner, facsimile, print, copy,  
232 scan, fax, document server

### 233 1.2 TOE Reference

234 The identification information of the TOE is shown below.

235 TOE Name: RICOH IM C2000 / C2500 / C3000 / C3500 / C4500 / C5500 / C6000

236 TOE Version: JE-1.10-H

237 TOE Type: Digital Multi-Function Printer (hereafter "MFP")

238 Target MFP models:

- 239 • RICOH IM C2000, IM C2000A, IM C2000F, and IM C2000G
- 240 • RICOH IM C2500, IM C2500A, IM C2500F, and IM C2500G
- 241 • RICOH IM C3000, IM C3000A, IM C3000F, and IM C3000G
- 242 • RICOH IM C3500, IM C3500A, IM C3500F, and IM C3500G
- 243 • RICOH IM C4500, IM C4500A, IM C4500F, and IM C4500G
- 244 • RICOH IM C5500, IM C5500A, and IM C5500F
- 245 • RICOH IM C6000, IM C6000F, and IM C6000G

246 All of the above MFPs are equipped with Printer, Scanner, and Copy functions, support an optional Fax function,  
247 and are upgraded to version JE-1.10-H software.

248 Additional options such as document feeders and finishers are available, but none affects the TSF.

249 The versions of the firmware and hardware corresponding to this version of the TOE are shown below. When  
250 using an MFP, you can display the firmware and hardware versions. The machine's serial number plate indicates  
251 which Type the model belongs to:

252 Type 1: MFPs for "-27", "-65", "-17", "-18" or "-29" models:

- 253 • RICOH IM C2000, RICOH IM C2000A, RICOH IM C2000G,  
254 RICOH IM C2500, RICOH IM C2500A, RICOH IM C2500G,  
255 RICOH IM C3000, RICOH IM C3000A, RICOH IM C3000G,  
256 RICOH IM C3500, RICOH IM C3500A, RICOH IM C3500G,
- 257 • SAVIN IM C2000, SAVIN IM C2000G,  
258 SAVIN IM C2500, SAVIN IM C2500G,  
259 SAVIN IM C3000, SAVIN IM C3000G,



- 260 SAVIN IM C3500, SAVIN IM C3500G,  
261 • LANIER IM C2000, LANIER IM C2000G,  
262 LANIER IM C2500, LANIER IM C2500G,  
263 LANIER IM C3000, LANIER IM C3000G,  
264 LANIER IM C3500, LANIER IM C3500G,  
265 • nashuatec IM C2000, nashuatec IM C2000A,  
266 nashuatec IM C2500, nashuatec IM C2500A,  
267 nashuatec IM C3000, nashuatec IM C3000A,  
268 nashuatec IM C3500, nashuatec IM C3500A,  
269 • Rex Rotary IM C2000, Rex Rotary C2000A,  
270 Rex Rotary C2500, Rex Rotary C2500A,  
271 Rex Rotary C3000, Rex Rotary C3000A,  
272 Rex Rotary C3500, Rex Rotary C3500A,  
273 • Gestetner IM C2000, Gestetner IM C2000A,  
274 Gestetner IM C2500, Gestetner IM C2500A,  
275 Gestetner IM C3000, Gestetner IM C3000A,  
276 Gestetner IM C3500, Gestetner IM C3500A,  
277

278 Type 2: MFPs for “-27”, “-65”, “-17”, “-18”, “-57” or “-29” models

- 279 • RICOH IM C4500, RICOH IM C4500A, RICOH IM C4500G,  
280 RICOH IM C5500, RICOH IM C5500A,  
281 RICOH IM C6000, RICOH IM C6000G,  
282 • SAVIN IM C4500, SAVIN IM C4500G,  
283 SAVIN IM C6000, SAVIN IM C6000G,  
284 • LANIER IM C4500, LANIER IM C4500G,  
285 LANIER IM C6000, LANIER IM C6000G,  
286 • nashuatec IM C4500, nashuatec IM C4500A,  
287 nashuatec IM C5500, nashuatec IM C5500A,  
288 nashuatec IM C6000,  
289 • Rex Rotary C4500, Rex Rotary C4500A,  
290 Rex Rotary C5500, Rex Rotary C5500A,  
291 Rex Rotary C6000,  
292 • Gestetner IM C4500, Gestetner IM C4500A,  
293 Gestetner IM C5500, Gestetner IM C5500A,  
294 Gestetner IM C6000  
295

296 Type 3: MFPs for “-00” or “-01” models

- 297 • RICOH IM C2000, RICOH IM C2000F  
298 RICOH IM C2500, RICOH IM C2500F  
299 RICOH IM C3000, RICOH IM C3000F  
300 RICOH IM C3500, RICOH IM C3500F  
301

302 Type 4: MFPs for “-00”, “-01” or “-04” models

- 303 • RICOH IM C4500, RICOH IM C4500A, RICOH IM C4500F  
304 RICOH IM C5500, RICOH IM C5500A, RICOH IM C5500F  
305 RICOH IM C6000, RICOH IM C6000F



306

307 Machine firmware and hardware for Type 1

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	Font EXP	1.00
	PCL	1.01
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.15
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
M2a_System	2.03.1	
M2a_BLEPlugin	4.0.1	

Primary Classification	Secondary Classification	Version
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00

Primary Classification	Secondary Classification	Version
	M2a_VoiceServ	2.01
	M2a_WEcoInfo	2.01
	M2a_WFaxInfo	2.00
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

308 (\*1): When the MFP includes Auto Reverse Document Feeder

309 (\*2): When the MFP includes One-Pass Duplex Scanning ADF

310 (\*3): When the MFP includes Exposure Glass Cover

311

312 Machine firmware and hardware for Type 2

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01

Primary Classification	Secondary Classification	Version
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	Font EXP	1.00
	PCL	1.01
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.15
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03.1
	M2a_BLEPlugin	4.0.1
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2

Primary Classification	Secondary Classification	Version
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00
	M2a_VoiceServ	2.01
	M2a_WEcolInfo	2.01
	M2a_WFaxInfo	2.00
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04

Primary Classification	Secondary Classification	Version
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

313 (\*1): When the MFP includes Auto Reverse Document Feeder

314 (\*2): When the MFP includes One-Pass Duplex Scanning ADF

315 (\*3): When the MFP includes Exposure Glass Cover

316

317 Machine firmware and hardware for Type 3

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	RPCS Font	1.00
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.21
	PSFont JIS2004	1.04
Option MSIS	0.38	

Primary Classification	Secondary Classification	Version
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03.1
	M2a_BLEPlugin	4.0.1
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00



Primary Classification	Secondary Classification	Version
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00
	M2a_VoiceServ	2.01
	M2a_WEcolInfo	2.01
	M2a_WFaxInfo	2.00
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04
ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)	
Hardware	Ic Ctlr	03
	Ic Key	01024704

318

319 Machine firmware and hardware for Type 4

Primary Classification	Secondary Classification	Version
Firmware	System/Copy	2.21
	Network Support	18.56

Primary Classification	Secondary Classification	Version
	Web Support	2.17
	Fax	02.02.00
	RemoteFax	02.01.00
	Scanner	02.02
	Web Uapl	2.01
	NetworkDocBox	2.01
	animation	2.01
	Printer	2.13
	RPCS	3.23.13
	RPCS Font	1.00
	IRIPS PS3	1.00
	IRIPS PDF	1.06
	IRIPS Font	1.21
	PSFont JIS2004	1.04
	Option MSIS	0.38
	GraphicData	2.00
	MovieData	1.00
	MovieData2	1.00
	MovieData3	1.00
	Data Erase Onb	1.05
	GWFCU3.8-22(WW)	04.00.00
	PowerSaving Sys	F.L3.23.1
	M2a_System	2.03.1
	M2a_BLEPlugin	4.0.1
	M2a_BluetoothSe	1.01
	M2a_cspf	3.00.00
	M2a_DeviceHub	2.01

Primary Classification	Secondary Classification	Version
	M2a_HelpService	6.01
	M2a_ICCdDisptch	3.07.00
	M2a_InstSetting	2.01
	M2a_iWnn	2.8.201
	M2a_iWnn_Hang	2.8.2
	M2a_iWnn_Hans	2.8.2
	M2a_iWnn_Hant	2.8.2
	M2a_KrbServ	1.07.01
	M2a_MeidaPrtScn	1.04
	M2a_NFCPlugin	3.03.00
	M2a_PrinterInfo	1.04
	M2a_PrinterSJob	1.03
	M2a_ProgramInfo	1.21
	M2a_QRCode_SDC	4.0.3
	M2a_QuickCdAuth	3.05.00
	M2a_RemAssist	1.1
	M2a_RemPnlOpe	1.2
	M2a_RemSptSvc	1.2
	M2a_SimpleWFD	1.17
	M2a_SmartCopy	1.07
	M2a_SmartFAX	5.08
	M2a_SmartScan	1.06
	M2a_SmartScanEx	2.02
	M2a_USBCdPlugin	3.03.00
	M2a_VoiceServ	2.01
	M2a_WEcoInfo	2.01
	M2a_WFaxInfo	2.00

Primary Classification	Secondary Classification	Version
	M2a_WLanguage	2.01
	M2a_WStopKey	2.00
	M2a_WTonner	2.00
	M2a_WTray	2.00
	M2a_zoo	3.02.00
	Engine	1.10:04
	ADF	01.000:03 (*1) 01.030:02 (*2) Blank (*3)
Hardware	Ic Ctlr	03
	Ic Key	01024704

320 (\*1): When the MFP includes Auto Reverse Document Feeder

321 (\*2): When the MFP includes One-Pass Duplex Scanning ADF

322 (\*3): When the MFP includes Exposure Glass Cover

323

### 324 1.3 TOE Variants

325 The models listed in Section 1.2 correspond to differences in print speed, and regional markets / localization. In  
 326 addition, some models are also marketed under different Ricoh Family Group brand names. A complete list of all  
 327 certified models is provided in the Notes for Administrators document identified in section 1.6.7.

328 All variants use the same hardware and the same versions of firmware for TOE security functions. All are  
 329 included in the scope of this Common Criteria certification, but only one representative model is tested (see  
 330 Section 1.4).

#### 331 1.3.1 Print speed variants

332 The first two numeric digits correspond to copy speed, e.g. C2000 performs 20 copies per minute, C2500  
 333 performs 25, and so on. Differences between models with different printing speeds are limited to print engine  
 334 components that do not affect the TSF.

#### 335 1.3.2 Regional variants

336 An alphabetic suffix corresponds to regional variations for default user interface languages and other  
 337 localization settings, and regional fonts and printer languages. There are no security-relevant differences  
 338 between regional variants.

#### 339 1.3.3 Branding variants

340 In addition to RICOH models (with no suffix or "A", "F", or "G" suffix), some models are marketed under the  
 341 following brand names; however, they have not been tested as part of the certification:

- 342     • SAVIN and LANIER (with no suffix or with “G” suffix)  
 343     • nashuatec, RexRotary, and Gestetner (with no suffix or with “A” suffix).

344 Differences between branding variants are limited to labels, displays, packaging materials, and documentation.  
 345 None of these differences affects the TSF.

346 **1.4 Evaluated and tested configurations**

347 The evaluated configuration comprises all of the required and optional TOE and non-TOE components listed in  
 348 the first two columns of the tables in subsections below. The specific components used for testing are identified  
 349 in the third column.

350 The tested configuration is equivalent to evaluated configurations because none of the variants for branding,  
 351 marketing region, paper speed, or paper feed, affects the TSF, and all variants employ the same TSF-enforcing  
 352 hardware and software.

353 The representative model selected for Common Criteria evaluation is a RICOH IM C4500, fitted with Fax Option  
 354 M37 for testing of fax-related security functions. The IM C4500 model was chosen because it is a high-speed  
 355 model that is marketed in all regions.

356 **1.4.1 Required TOE components**

357 The following TOE components are required to perform basic security functions of a hardcopy device.

Function	Required TOE component(s)	Tested TOE components
Hardware	Any of the models specified in Section 1.2 and 1.3	RICOH IM C4500 D0BN-17
Software	Version JE-1.10-H software upgrade	Version JE-1.10-H software upgrade

358 *Table 1 Required TOE components*

359 **1.4.2 Optional TOE components**

360 Optional security functions require additional TOE components, listed in Table 2:

Security function	Optional TOE components	Tested TOE components
Fax-network separation	Fax Control Unit (FCU)	Fax Control Unit Type M37

361 *Table 2 Optional TOE components*

362 **1.4.3 Required non-TOE components**

363 The following non-TOE components are required for the TOE to perform basic security functions of a hardcopy  
 364 device.

Security function	Required non-TOE component(s)	Tested TOE components
Trusted communications	Connection to a local area network	Yes
Audit log collection	Connection to an audit log server on the LAN	syslog server

365 *Table 3 Required non-TOE components*

366 **1.4.4 Optional non-TOE components**

367 Optional security functions require additional non-TOE components, listed in Table 4:

Security function	Optional non-TOE component(s)	Tested TOE components
Fax-network separation, fax-related security functions	Connection to a telephone line	PSTN emulator, PC with fax driver for sending, fax machine for receiving

Security function	Optional non-TOE component(s)	Tested TOE components
Network-based identification and authentication	Connection to an authentication server on the LAN	LDAP server
Protection of scanner output on network	Connection to an SMTP server on the LAN	SMTP server

368 Table 4 Optional non-TOE components

369 **1.5 TOE Overview**

370 This section defines TOE Type, TOE Usage and Major Security Features of TOE.

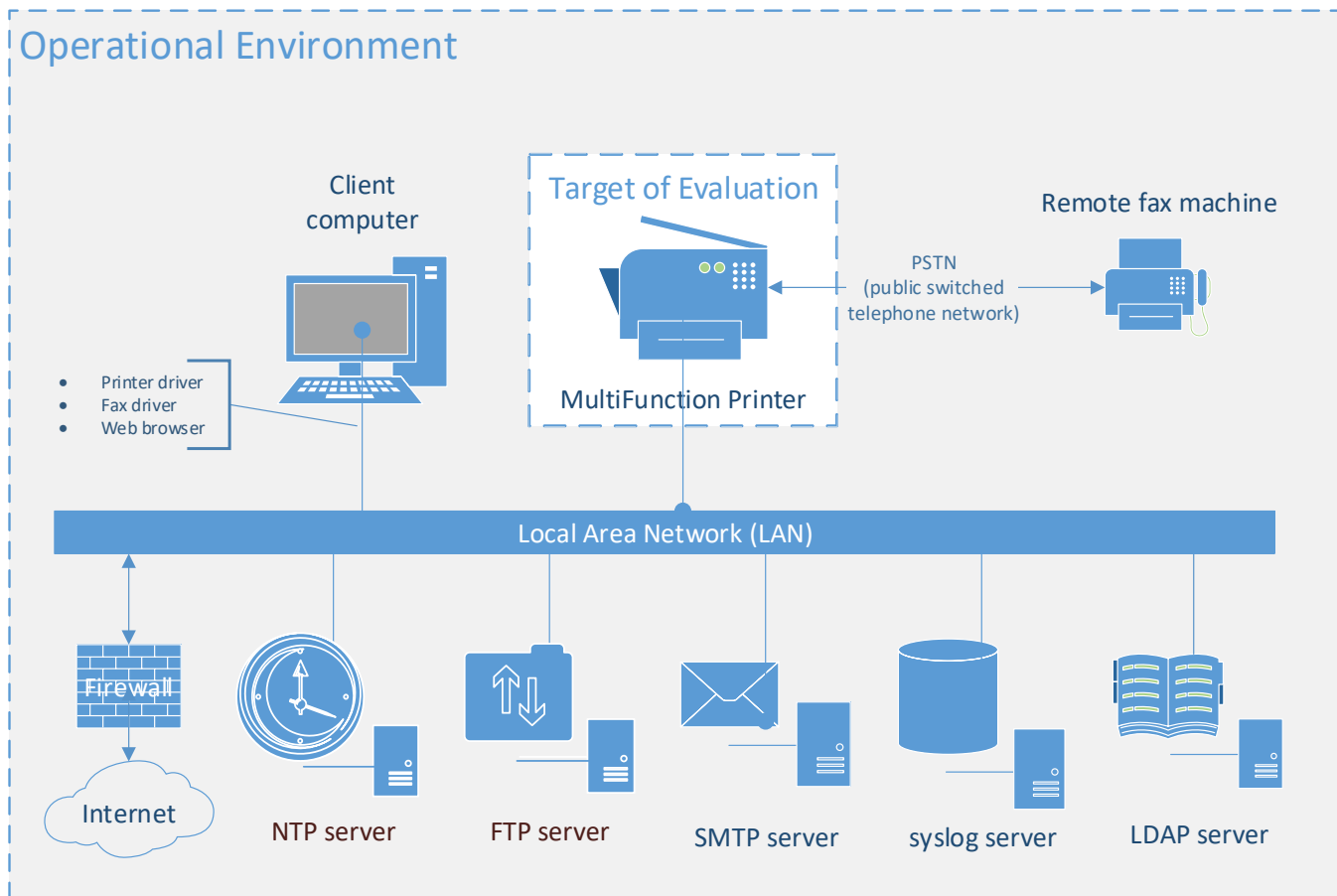
371 **1.5.1 TOE Type**

372 This TOE is a Digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs  
 373 electronic and hardcopy documents.

374 **1.5.2 TOE Usage**

375 The operational environment of the TOE is illustrated below and the usage of the TOE is outlined in this section.

376 As shown in Figure 1, the TOE is connected to its operational environment through a local area network  
 377 (hereafter "LAN") and the public switched telephone network (PSTN). Other elements of the TOE's operational  
 378 environment include a remote fax machine, an SMTP server, an Audit Server, and a user's client computer. Users  
 379 can operate the TOE from the Operation Panel of the TOE or through LAN communications. Each element is  
 380 described in this section.



381

382 *Figure 1 Example of TOE Environment*

### 383 1.5.2.1 Multifunction Printer (MFP)

384 It is the TOE. Users can perform the following operations from the Operation Panel of the MFP:

- 385 • Configuration of the MFP,
- 386 • Copying, faxing, storage, and network transmission of paper documents,
- 387 • Printing, faxing, network transmission, and deletion of the stored documents.
- 388 • Receiving fax documents via telephone lines and storing them as documents.

### 389 1.5.2.2 LAN

390 Network used in the TOE environment.

### 391 1.5.2.3 Client computer

392 A computer that performs as a client of the TOE via the LAN. Users can remotely operate the MFP from the  
393 client computer:

- 394 • Various settings for the MFP using a Web browser installed on the client computer,
- 395 • Operation of stored documents using a Web browser installed on the client computer,
- 396 • Storage and/or printing of documents using the printer driver installed on the client computer,
- 397 • Faxing documents using the fax driver installed on the client computer.

### 398 1.5.2.4 PSTN line

399 A connection to a public switched telephone network for the TOE to communicate with external fax machines.

### 400 1.5.2.5 Firewall

401 A device to protect the LAN from Internet threats.

### 402 1.5.2.6 SMTP Server

403 An external IT entity used by the TOE for e-mail transmission.

### 404 1.5.2.7 syslog Server

405 An external IT entity used by the TOE for audit log storage.

### 406 1.5.2.8 LDAP server

407 An external IT entity used by the TOE for network authentication of users.

### 408 1.5.2.9 FTP server

409 An external IT entity used by the TOE to receive and store user documents.

## 410 1.5.3 Major Security Features of TOE

411 The TOE stores documents in it, and sends and receives documents to and from the IT devices connected to the  
412 LAN. To ensure provision of confidentiality and integrity for those documents, the TOE has the following security  
413 features:

- 414 • Identification and Authentication
- 415 • Use-of-Feature Authorization
- 416 • Access Control
- 417 • Stored Data Encryption
- 418 • Trusted Communications



- 419       • Administrative Roles
- 420       • Auditing
- 421       • Trusted Operation
- 422       • PSTN Fax-Network Separation

## 423   1.6 TOE Description

424   This section describes the Physical Boundary of TOE, Hardware components, Logical Boundary of TOE, TOE  
425   Functions, and Guidance Documents.

### 426   1.6.1 Physical Boundary of TOE

427   The physical boundary of the TOE is the MFP, which consists of the following hardware components (shown in  
428   Figure 2): Operation Panel Unit, Engine Unit, (optional) Fax Controller Unit, Controller Board, HDD, Ic Ctlr,  
429   Network Unit, USB Port, and SD Card Slot. The MFP also consists of software components. These components  
430   comprise a physically large product that is delivered at once by a delivery company to users, and it is often set  
431   up with the assistance of a customer engineer.

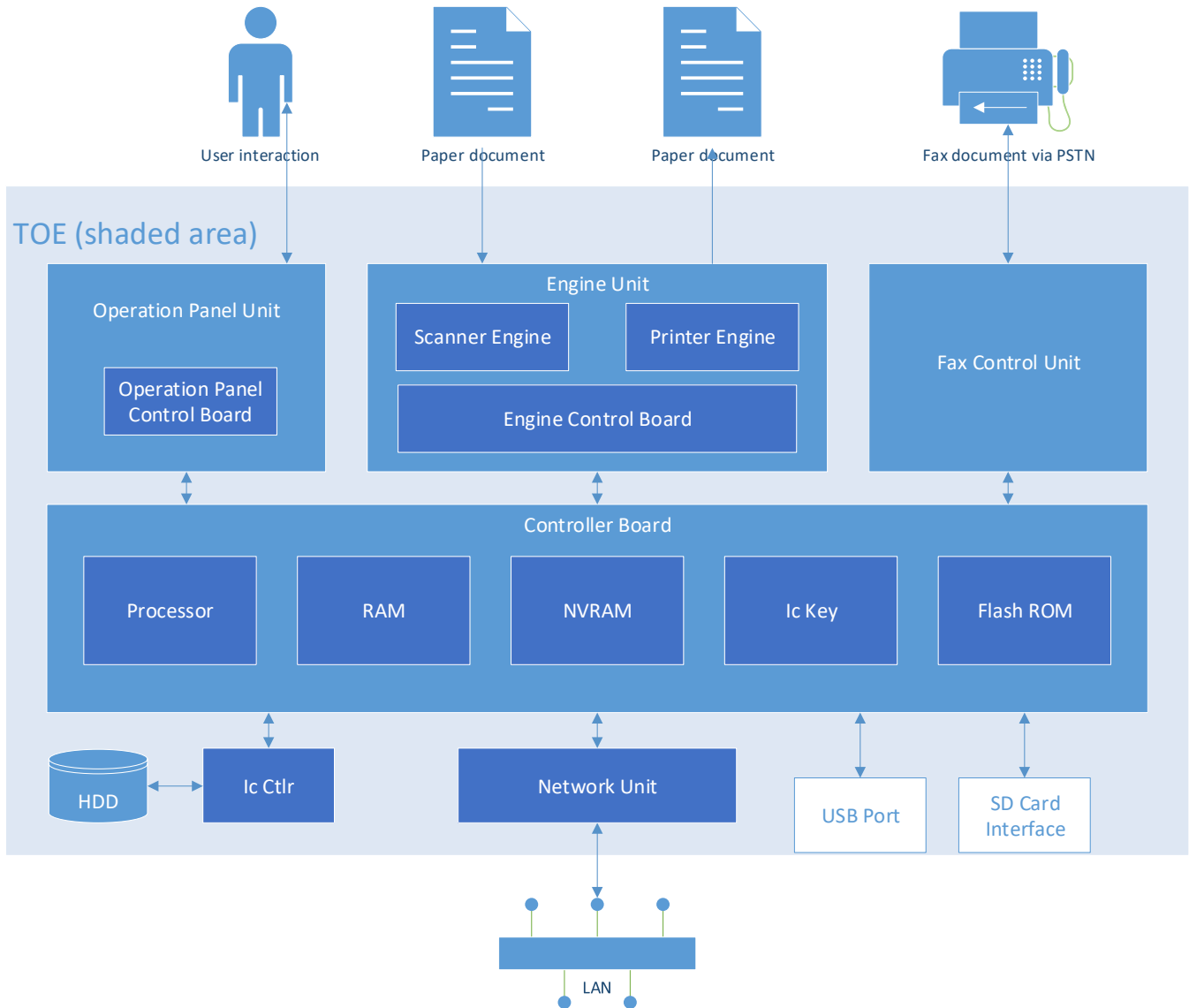


Figure 2 Hardware Configuration of the TOE

432

433

## 434 1.6.2 Hardware components

### 435 1.6.2.1 Controller Board

436 The Controller Board is a device that contains Processors, RAM, NVRAM, Ic Key, and FlashROM. The Controller  
 437 Board sends and receives information to control the MFP. The information is processed by the MFP Control  
 438 Software. The following describes the components of the Controller Board:

#### 439 1.6.2.1.1 Processor

440 A semiconductor chip that performs basic computer processing for MFP operations.

#### 441 1.6.2.1.2 RAM

442 A volatile memory medium which is used as a working area for image processing such as  
 443 compressing/decompressing the image data. It is also used to temporarily read and write internal information.

444 **1.6.2.1.3 NVRAM**

445 A non-volatile memory medium in which TSF data for configuring MFP operations is stored. The NVRAM is a  
446 field-replaceable non-volatile storage device, and is claimed as such in this document.

447 **1.6.2.1.4 Ic Key**

448 A hardware security module which provides true random number generation and protected storage.

449 **1.6.2.1.5 FlashROM**

450 A non-volatile memory medium in which the MFP Control Software is installed.

451 **1.6.2.2 Operation Panel**

452 The Operation Panel consists of an LCD touch screen user interface and LED indicators that are controlled by  
453 Operation Panel Control Software installed on the Operation Panel Control Board. The Operation Panel Control  
454 Software performs the following:

- 455     1. Transfers operation instructions from the LCD touch screen to the Controller Board.  
456     2. Controls the LED indicators and displays information on the LCD touch screen according to display  
457         instructions from the MFP Control Software.

458 The Operation Panel utilizes Linux 3.18 on an ARM Cortex-A9 Quad Core processor.

459 **1.6.2.3 Engine Unit**

460 The Engine Unit consists of a Scanner Engine which scans paper documents, and a Printer Engine that prints and  
461 ejects paper documents, both controlled by the Engine Control Software installed on the Engine Control Board.  
462 The Engine Control Software sends status information about the Scanner Engine and Printer Engine to the  
463 Controller Board, and operates the Scanner Engine or Printer Engine according to instructions from the MFP  
464 Control Software.

465 **1.6.2.4 Fax Controller Unit (FCU)**

466 The Fax Controller Unit consists of a modem which sends and receives fax data to and from other fax devices  
467 using the G3 standard for communication. FCU Control Software is installed on the Fax Controller Unit operates  
468 the modem and exchanges fax data according to instructions from the MFP Control Software. The Fax Controller  
469 Unit type M37 utilizes the RU30 processor in its operation.

470 **1.6.2.5 HDD**

471 The HDD is a hard disk drive that is a non-volatile memory medium. It stores documents, login user names and  
472 login passwords of Normal Users. The HDD is a field-replaceable non-volatile storage device, and is claimed as  
473 such in this document.

474 **1.6.2.6 Ic Ctlr**

475 The Ic Ctlr is a board that implements data encryption and decryption functions for data stored on the HDD.

476 **1.6.2.7 Network Unit**

477 The Network Unit is an external interface to an Ethernet LAN.

478 **1.6.2.8 USB Port**

479 The USB Port is an external interface to connect a client computer to the TOE for printing directly from the client  
480 computer. During installation, this interface is disabled.

481 1.6.2.9 SD Card Slot  
 482 There are two SD Card Slots, one for customer engineers and one for users.

483 The SD Card Slot for customer engineer is used when the customer engineer installs the TOE. A cover is placed  
 484 on the SD Card Slot during the TOE operation so that an SD Card cannot be inserted into or removed from the  
 485 slot.

486 The SD Card Slot for users is used by users to print documents in the SD Card. The slot is set to disabled at the  
 487 installation.

488 **1.6.3 Logical Boundary of the TOE**

489 The Basic Functions and Security Functions are described as follows:

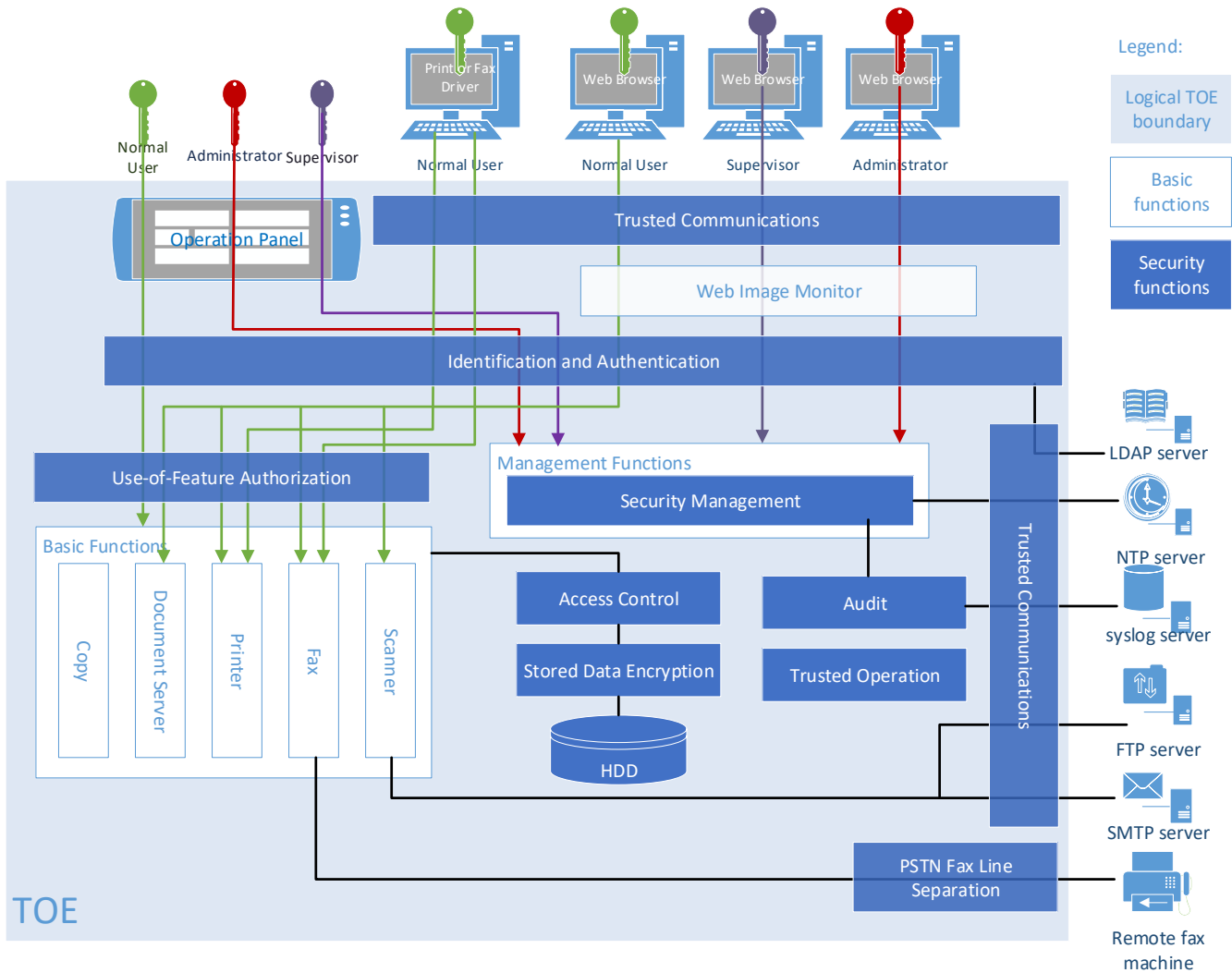


Figure 3 Logical Boundary of the TOE

490  
 491  
 492 **1.6.4 Basic Functions**

493 1.6.4.1 Copy Function

494 The Copy Function scans paper documents to be printed.

495 *1.6.4.2 Printer Function*

496 The Printer Function prints or stores documents received from a printer driver installed on the client computer,  
497 and prints or deletes previously-stored documents from commands from the Operation Panel or the client  
498 computer's web browser.

499 *1.6.4.3 Scanner Function*

500 The Scanner Function scans paper documents and then transmits and deletes the scanned images, on command  
501 from the Operation Panel.

502 *1.6.4.4 Fax Function*

503 The Fax Function consists of a Fax Transmission Function and a Fax Reception Function. Both functions exchange  
504 documents according to the Group 3 standard over a Public Switch Telephone Network (PSTN).

505 The Fax Transmission Function sends scanned images of paper documents, or images of electronic documents  
506 from a client computer, to external fax devices.

507 The Fax Reception Function receives documents from external fax devices, and stores them in the TOE.

508 *1.6.4.5 Document Server Function*

509 The Document Server Function is to perform operations on persistently-stored documents in the TOE.

510 From the Operation Panel, users can store, print and delete Document Server documents.

511 From a client computer, users can print and delete Document Server documents.

512 *1.6.4.6 Management Function*

513 The Management Function allows authorized users to configure the TOE's operation. The management function  
514 can be accessed from the Operation Panel or a client computer. Security Management functions can be  
515 accessed only by Administrators.

516 *1.6.4.7 Web Image Monitor Function*

517 The Web Image Monitor Function (hereafter "WIM") allows authorized users to remotely control the TOE from a  
518 web browser on a client computer.

519 **1.6.5 Security Functions**

520 The Security Functions are described as follows:

521 *1.6.5.1 Identification and Authentication*

522 User identification, authentication, and authorization ensure that functions of the TOE are accessible only to  
523 Users who have been authorized by an Administrator. User identification and authentication is also used as the  
524 basis for access control and administrative roles and helps associate security-relevant events and TOE use with  
525 specific Users. Identification and authentication is performed by the TOE. User's credentials can be entered  
526 locally on the Operation Panel, through WIM login, through print or fax drivers, or using network authentication  
527 services.

528 *1.6.5.2 Use-of-Feature Authorization*

529 The Use-of-Feature Restriction Function authorizes authenticated users to perform the operations of Copy  
530 Function, Printer Function, Scanner Function, Document Server Function and Fax Function, based on the user  
531 role and the permissions set by an Administrator for each user.

532 **1.6.5.3 Access Control**

533 Access controls ensure that documents, document processing job information, and security-relevant data, are  
534 accessible only to authenticated users who have appropriate access permissions.

535 **1.6.5.4 Stored Data Encryption**

536 The Stored Data Protection Function encrypts data on the HDD and in NVRAM to protect documents and  
537 confidential system information if those devices are removed from the TOE. Keychains for both devices are  
538 described in this document.

539 **1.6.5.5 Trusted Communications**

540 Trusted communication paths are established to ensure that communications with the TOE are performed with  
541 known endpoints. Data encryption ensures that data assets cannot be accessed while in transit on the LAN.

542 **1.6.5.6 Administrative Roles**

543 Role-based access controls ensure that the ability to configure the security settings of the TOE is available only  
544 to Users who have been authorized with an Administrator role.

545 **1.6.5.7 Auditing**

546 Audit logs are generated by the TOE to ensure that security-relevant events and TOE use can be monitored by  
547 authorized personnel. The TOE generates audit logs and securely transmits them to an External IT entity for  
548 storage. While stored in the TOE, audit logs are protected from unauthorized access and modification.

549 **1.6.5.8 Trusted Operation**

550 The Software Verification Function verifies the integrity and authenticity of MFP Control Software, FCU Control  
551 Software, and Operation Panel Control Software, before applying updates. Power-on self-tests are performed to  
552 ensure that TOE operation is not disrupted by detectable malfunction.

553 **1.6.5.9 PSTN Fax-Line Separation**

554 The Fax Line Separation Function restricts information received from or transmitted to the telephone network to  
555 only fax data and fax protocols. It ensures that the fax modem cannot be used to bridge to the LAN.

556 **1.6.5.10 Image Overwrite**

557 The Image Overwrite Function actively overwrites residual image data stored on the HDD after a Document  
558 Processing job has been completed or cancelled.

559 **1.6.6 Functions supported but not evaluated**

560 The following functions supported by the TOE are not included in this evaluation:

- 561 • Fax over IP
- 562 • Store while copying documents
- 563 • Store while sending documents by fax
- 564 • Menu Protect
- 565 • PDF Group Passwords
- 566 • SMTP Authentication
- 567 • File Transfer Authentication
- 568 • Erase All Memory

569 **1.6.7 Guidance Documents**

570 A common set of guidance documents is provided for the TOE. Selection of a particular guidance document set  
571 depends on the print speed and sales region, and they are identified in the Notes for Administrators document.

572 Paper manuals supplied with the TOE:

- 573 • Safe Use of This Machine
- 574 • For Users of This Product
- 575 • Notes for Users
- 576 • Software License Agreement

577 Online manuals available for the TOE:

- 578 • Safety Information
- 579 • User Guide
  - 580 ○ Setup
  - 581 ○ Introduction and Basic Operations
  - 582 ○ Copy
  - 583 ○ Document Server
  - 584 ○ Fax
  - 585 ○ Scan
  - 586 ○ Printer
  - 587 ○ Maintenance
  - 588 ○ Troubleshooting
  - 589 ○ Settings
  - 590 ○ Specifications
  - 591 ○ Security
  - 592 ○ Driver Installation Guide
- 593 • Security Reference
- 594 • Notes for Administrators v1.1: Using This Machine in a Network Environment Compliant with Protection  
595 Profile for Hardcopy Devices PP\_HCD\_V1.0

596 A complete list of manuals as they apply to all TOE variants is provided in the Notes for Administrators  
597 document. URLs for online manuals are provided in the paper manual, Safe Use of This Machine, which is  
598 supplied with the TOE.



599 **2 ST Conformance Claims (ASE\_CCL)**

600 **2.1 Common Criteria (CC) conformance claims**

601 The CC conformance claim of this ST and TOE is as follows:

- 602 • Part 1: Introduction and general model Version 3.1 Revision 5 CCMB-2017-04-001
- 603 • Part 2: Security functional components Version 3.1 Revision 5 CCMB-2017-04-002 extended
- 604 • Part 3: Security assurance components Version 3.1 Revision 5 CCMB-2017-04-003 conformant (EAL1)

605 **2.2 Protection Profile (PP) conformance claims**

606 The PP to which this ST and TOE are strictly conformant and exactly compliant is:

- 607 • PP Name: Protection Profile for Hardcopy Devices
- 608 • PP Version: 1.0, dated 2015-09-11

609 The ST and TOE also address all of the NIAP Technical Decisions that apply to the PP:

- 610 • TD0074 FCS\_CKM.1(a) Requirement in HCD PP v1.0
- 611 • TD0157 FCS\_IPSEC\_EXT.1.1 - Testing SPDs
- 612 • TD0176 FDP\_DSK\_EXT.1.2 - SED Testing
- 613 • TD0219 NIAP Endorsement of Errata for HCD PP v1.0 (Errata #1, June 2017)
- 614 • TD0253 Assurance Activities for Key Transport
- 615 • TD0261 Destruction of CSPs in flash
- 616 • TD0299 Update to FCS\_CKM.4 Assurance Activities
- 617 • TD0393 Require FTP\_TRP.1(b) only for printing
- 618 • TD0474 Removal of Mandatory Cipher Suite in FCS\_TLS\_EXT.1

619 Hereafter, the PP and applicable Technical Decisions are referred to collectively as “HCD PP v1.0”.

620 The TOE claims conformance with the following essential, additional, and optional uses as specified in the PP:

Category	Features	Conformance
<b>Essential Uses</b>	Scanning	Claimed
	Printing	Claimed
	Copying	Claimed
	Network Communications	Claimed
	Administration	Claimed
<b>Additional Uses</b>	PSTN Faxing	Claimed
	Storage and Retrieval	Claimed
	Field-Replaceable Nonvolatile Storage	Claimed
<b>Optional Uses</b>	Internal Audit Log Storage	Claimed
	Image Overwrite	Claimed
	Purge Data	Not Claimed

621 *Table 5 Protection Profile claims*

622 **2.3 Conformance Claim Rationale**

623 **2.3.1.1 Consistency Claim with TOE Type in this PP**

624 In this PP, a conforming product must support at least one of the job functions printing, scanning, or copying  
625 and must support the functions network communications and administration.

626 The TOE is a product that supports printing, scanning, copying, network communications, and administration  
627 functions, as required by the PP.

628 **2.3.2 Consistency Claim with Security Problems and Security Objectives in PP**

629 The TOE is exactly compliant with the Security Problems and Security Objectives in this PP.

630 **2.3.3 Consistency Claim with Security Requirements in PP**

631 The TOE is exactly compliant with the Security Requirements in this PP.

### 3 Security Problem Definitions (ASE\_SPD)

This section describes Threats, Organizational Security Policies and Assumptions.

#### 3.1 Users

There are two categories of Users defined in this ST, Normal and Admin. There are two Admin sub-roles.

Designation	Name	Definition
<b>U.NORMAL</b>	Normal User	A User who has been identified and authenticated and does not have an administrative role
<b>U.ADMIN</b>	Administrator	A User who has been identified and authenticated and has an administrative role
<b>U.ADMIN.SUP</b>	MFP Supervisor	
<b>U.ADMIN.MFP</b>	MFP Administrator	

Table 6 User categories

A pseudo-user role, Customer Engineer, can be enabled by an Administrator for use by an authorized service representative. It is normally disabled, as it is in the evaluated configuration.

#### 3.2 Assets

Assets are passive entities in the TOE that contain or receive information. In this PP, Assets are Objects (as defined by the CC). There are two categories of Assets defined in this PP:

Designation	Asset category	Definition
<b>D.USER</b>	User Data	Data created by and for Users that do not affect the operation of the TSF
<b>D.TSF</b>	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

Table 7 Asset categories

There are no additional Asset categories defined in this ST.

##### 3.2.1 User Data

User Data are composed of two types:

Designation	User Data type	Definition
<b>D.USER.DOC</b>	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
<b>D.USER.JOB</b>	User Job Data	Information related to a User's Document or Document Processing Job

Table 8 User Data types

There are no additional types of User Data defined in this ST. Attributes associate documents and document processing jobs with the document processing functions of the TOE:

Document processing function	Attribute
Printing	+PRT
Copying	+CPY
Scanning	+SCN
Document Storage/Retrieval	+DSR
Fax (reception)	+FAXIN
Fax (transmission)	+FAXOUT

Table 9 Document and Job Attributes

650 **3.2.2 TSF Data**

651 TSF Data are composed of two types:

Designation	TSF Data type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

652 *Table 10 TSF Data types*

653 There are no additional types of TSF Data defined in this ST.

654 **3.2.2.1 Protected TSF Data**

655 D.TSF.PROT is composed of the following data:

Data item
Login user name
Number of Attempts before Lockout
Settings for Lockout Release Timer
Lockout time
Date settings (year/month/day)
Time settings
Minimum Character No.
Password Complexity Setting
Operation Panel auto logout time
WIM auto logout time
Stored Reception File User
Document user list
Available function list
User authentication method
Device Certificate
Network settings
Audit transfer settings
TOE Software

656 *Table 11 Data in D.TSF.PROT*

657 **3.2.2.2 Confidential TSF Data**

658 In this ST, D.TSF.CONF is composed of the following data:

Data item
Login password
Audit log
HDD cryptographic key

659 *Table 12 Data in D.TSF.CONF*

660 **3.3 Threat definitions**

661 The following threats are mitigated by this TOE:

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

662 *Table 13 Threats*

663 **3.4 Organizational Security Policies**

664 The following Organizational Security Policies (OSPs) are enforced by this TOE:

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL (conditionally mandatory)	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.

665 *Table 14 Organizational Security Policies*

666 **3.5 Assumptions**

667 The following assumptions must be satisfied in order for the Security Objectives and Security Functional  
 668 Requirements to be effective:

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

669 *Table 15 Assumptions*

670 **4 Security Objectives (ASE\_OBJ)**

671 **4.1 Security Objectives for the TOE**

672 The following Security Objectives are satisfied by this TOE:

Designation	Definition
O.USER_I&A	The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.
O.ACCESS_CONTROL	The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
O.USER_AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of software updates.
O.TSF_SELF_TEST	The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.
O.COMMS_PROTECTION	The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.
O.AUDIT	The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE.
O.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.
O.KEY_MATERIAL (conditionally mandatory)	The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.
O.FAX_NET_SEPARATION (conditionally mandatory)	If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function.
O.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data in its Field-Replaceable Nonvolatile Storage Devices.

673 *Table 16 Security Objectives for the TOE*

674 **4.2 Security Objectives for the Operational Environment**

675 The following Security Objectives must be satisfied by the TOE’s Operational Environment.

Designation	Definition
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer’s guidance to correctly configure the TOE and protect passwords and keys accordingly.

676 *Table 17 Security Objectives for the Operational Environment*

677  
678

### 4.3 Security Objectives rationale

The following table maps threats, OSPs, and assumptions, to their respective Security Objectives.

Threat/Policy/Assumption	Rationale
T.UNAUTHORIZED_ACCESS <i>An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.</i>	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_COMPROMISE <i>An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.</i>	O.ACCESS_CONTROL restricts access to TSF Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_FAILURE <i>A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.</i>	O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.
T.UNAUTHORIZED_UPDATE <i>An attacker may cause the installation of unauthorized software on the TOE.</i>	O.UPDATE_VERIFICATION verifies the authenticity of software updates.
T.NET_COMPROMISE <i>An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.</i>	O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks.
P.AUTHORIZATION <i>Users must be authorized before performing Document Processing and administrative functions.</i>	O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users. O.USER_I&A provides the basis for authorization. O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.
P.AUDIT <i>Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.</i>	O.AUDIT requires the generation of audit data. O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users. O.USER_AUTHORIZATION provides the basis for authorization.
P.COMMS_PROTECTION <i>The TOE must be able to identify itself to other devices on the LAN.</i>	O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.
P.STORAGE_ENCRYPTION (conditionally mandatory) <i>If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.</i>	O.STORAGE_ENCRYPTION protects User Document Data and Confidential TSF Data stored in Field-Replaceable Nonvolatile Storage Devices from exposure if a device has been removed from the TOE and its Operational Environment.
P.KEY_MATERIAL (conditionally mandatory) <i>Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.</i>	O.KEY_MATERIAL protects keys and key materials from unauthorized access and ensures that they any key materials are not stored in cleartext on the device that uses those materials for its own encryption.
P.FAX_FLOW (conditionally mandatory) <i>If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.</i>	O.FAX_NET_SEPARATION requires a separation between the PSTN fax line and the LAN.

Threat/Policy/Assumption	Rationale
P.IMAGE_OVERWRITE (optional) <i>Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.</i>	O.IMAGE_OVERWRITE overwrites residual image data from Field-Replaceable Nonvolatile Storage Devices after Document Processing jobs are completed or cancelled.
A.PHYSICAL <i>Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.</i>	OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE.
A.NETWORK <i>The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.</i>	OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE.
A.TRUSTED_ADMIN <i>TOE Administrators are trusted to administer the TOE according to site security policies.</i>	OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.TRAINED_USERS <i>Authorized Users are trained to use the TOE according to site security policies.</i>	OE.ADMIN_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Administrators. OE.USER_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Users.

679 Table 18 Security Objectives rationale



680 **5** Extended Component Definitions (ASE\_ECD)

681 This ST uses extended components that are defined in HCD PP v1.0 and in the claimed Technical Decisions and  
682 Errata. No additional extended components are defined for this ST.

## 6 Security Functional Requirements (ASE\_REQ)

### 6.1 Notational conventions

**Bold** typeface indicates the portion of an SFR that has been completed or refined in the Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition.

*Italic* typeface indicates the portion of an SFR that has been completed for this Security Target.

***Bold italic*** typeface indicates the portion of an SFR that has been partially completed or refined in the Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition, and which also has been completed for this Security Target.

SFR components that are followed by a letter in parentheses, e.g., (a), (b), ..., represent required iterations. This Security Target uses the iteration identifiers that are used in the Protection Profile; therefore, they may not be sequential in this Security Target.

SFR components that are followed by an identifier in square brackets, e.g., [1], [2]..., represent iterations that have been added for this Security Target. In some cases, they may be combined with the (letter) designation of required iterations, e.g., FCS\_COP.1 (d)[1], FCS\_COP.1 (d)[2], ... .

Extended components are identified by “\_EXT” following the SFR name.

### 6.2 Class FAU: Security Audit

#### 6.2.1 FAU\_GEN.1 Audit data generation

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT\_STM.1 Reliable time stamps

**FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the **not specified** level of audit; and
- c) **All auditable events specified in Table 19**, [*no other specifically defined auditable events*].

**FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 19**, [*no other audit relevant information*].

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None

Auditable event	Relevant SFR	Additional information
Failure to establish session.	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure.

713 *Table 19 Auditable Events*

714 **Application Note:**

715 *In cases where user identification events are inseparable from user authentication events, they may be*  
 716 *considered to be a single event for audit purposes.*

717 *Regarding FMT\_SMR.1, if the relationship between users and roles is not modifiable, its auditable event*  
 718 *cannot be generated and the requirement to generate an audit record can be ignored.*

719 *The ST author can include other auditable events directly in the table; they are not limited to the list*  
 720 *presented.*

721 **Assurance Activity:**

722 *TSS:*

723 The evaluator shall check the TOE Summary Specification (TSS) to ensure that auditable events and its  
 724 recorded information are consistent with the definition of the SFR.

725 *Operational Guidance:*

726 The evaluator shall check the guidance documents to ensure that auditable events and its recorded  
 727 information are consistent with the definition of the SFRs.

728 *Test:*

729 The evaluator shall also perform the following tests:

730 The evaluator shall check to ensure that the audit record of each of the auditable events described in  
 731 Table 19 is appropriately generated.

732 The evaluator shall check a representative sample of methods for generating auditable events, if there are  
 733 multiple methods.

734 The evaluator shall check that FIA\_UAU.1 events have been generated for each mechanism, if there are  
 735 several different I&A mechanisms.

736 **6.2.2 FAU\_GEN.2 User identity association**

737 (for O.AUDIT)

738 Hierarchical to: No other components.

739 Dependencies: FAU\_GEN.1 Audit data generation

740 FIA\_UID.1 Timing of identification

741 **FAU\_GEN.2.1** For audit events resulting from actions of identified users, the TSF shall be able to associate each  
 742 auditable event with the identity of the user that caused the event.

743 **Assurance Activity:**

744 The Assurance Activities for FAU\_GEN.1 address this SFR.

### 745 6.2.3 FAU\_SAR.1 Audit review

746 (for O.AUDIT)

747 Hierarchical to: No other components.

748 Dependencies: FAU\_GEN.1 Audit data generation

749 **FAU\_SAR.1.1** The TSF shall provide [**U.ADMIN**] with the capability to read all records from the audit records.

750 **FAU\_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the  
751 information.

#### 752 **Assurance Activity:**

753 The following assurance activities are required when storing audit records inside the TOE.

754 *TSS:*

755 The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed  
756 only by authorized users and functions to view audit records.

757 The evaluator shall check to ensure that the TSS contains a description of the methods of using interfaces  
758 that retrieve audit records (e.g., methods for user identification and authentication, authorization, and  
759 retrieving audit records).

760 *Operational Guidance:*

761 The evaluator shall check to ensure that the operational guidance appropriately describes the ways of  
762 viewing audit records and forms of viewing.

763 *Test:*

764 The evaluator shall also perform the following tests:

- 765 1. The evaluator shall check to ensure that the forms of audit records are provided as specified in  
766 the operational guidance by retrieving audit records in accordance with the operational guidance.
- 767 2. The evaluator shall check to ensure that no users other than authorized users can retrieve audit  
768 records.
- 769 3. The evaluator shall check to ensure that all audit records are retrieved by the operation of  
770 retrieving audit records.

### 771 6.2.4 FAU\_SAR.2 Restricted audit review

772 (for O.AUDIT)

773 Hierarchical to: No other components.

774 Dependencies: FAU\_SAR.1 Audit review

775 **FAU\_SAR.2.1** The TSF shall prohibit all users read access to the audit records, except those users that have been  
776 granted explicit read-access.

#### 777 **Assurance Activity:**

778 *Test:*

779 The evaluator shall include tests related to this function in the set of tests performed in FMT\_SMF.1.

#### 780 6.2.5 FAU\_STG.1 Protected audit trail storage

781 (for O.AUDIT)

782 Hierarchical to: No other components.

783 Dependencies: FAU\_GEN.1 Audit data generation

784 **FAU\_STG.1.1** The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

785 **FAU\_STG.1.2** The TSF shall be able to prevent unauthorised modifications to the stored audit records in the  
786 audit trail.

#### 787 **Assurance Activity:**

788 The following assurance activities are required when storing audit records inside the TOE.

789 *TSS:*

790 The evaluator shall check to ensure that the TSS contains a description of the means of preventing audit  
791 records from unauthorized access (modification, deletion).

792 *Operational Guidance:*

793 The evaluator shall check to ensure that the TSS and operational guidance contain descriptions of the  
794 interfaces to access to audit records, and if the descriptions of the means of preventing audit records  
795 from unauthorized access (modification, deletion) are consistent.

796 *Test:*

797 The evaluator shall also perform the following test:

798 1. The evaluator shall test that an authorized user can access the audit records.

799 2. The evaluator shall test that a user without authorization for the audit data cannot access the audit  
800 records.

#### 801 6.2.6 FAU\_STG\_EXT.1 Extended: External Audit Trail Storage

802 (for O.AUDIT)

803 Hierarchical to: No other components.

804 Dependencies: FAU\_GEN.1 Audit data generation,

805 FTP\_ITC.1 Inter-TSF trusted channel.

806 **FAU\_STG\_EXT.1.1** The TSF shall be able to transmit the generated audit data to an External IT Entity using a  
807 trusted channel according to FTP\_ITC.1.

#### 808 **Assurance Activity:**

809 *TSS:*

810 The evaluator shall examine the TSS to ensure it describes the means by which the audit data are  
811 transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted  
812 channel mechanism will be performed as specified in the associated assurance activities for the particular  
813 trusted channel mechanism.

814 The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored  
815 locally; what happens when the local audit data store is full; and how these records are protected against  
816 unauthorized access. The evaluator shall also examine the operational guidance to determine that it  
817 describes the relationship between the local audit data and the audit data that are sent to the audit log  
818 server. For example, when an audit event is generated, is it simultaneously sent to the external server and  
819 the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the  
820 audit server.

821 *Operational Guidance:*

822 The evaluator shall also examine the operational guidance to ensure it describes how to establish the  
823 trusted channel to the audit server, as well as describe any requirements on the audit server (particular  
824 audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed  
825 to communicate with the audit server.

826 *Test:*

827 The evaluator shall perform the following test for this requirement:

828 Test 1: The evaluator shall establish a session between the TOE and the audit server according to the  
829 configuration guidance provided. The evaluator shall then examine the traffic that passes between the  
830 audit server and the TOE during several activities of the evaluator’s choice designed to generate audit  
831 data to be transferred to the audit server. The evaluator shall observe that these data are not able to be  
832 viewed in the clear during this transfer, and that they are successfully received by the audit server. The  
833 evaluator shall record the particular software (name, version) used on the audit server during testing.

#### 834 6.2.7 FAU\_STG.4 Prevention of audit data loss

835 (for O.AUDIT)

836 Hierarchical to: FAU\_STG.3 Action in case of possible audit data loss

837 Dependencies: FAU\_STG.1 Protected audit trail storage

838 **FAU\_STG.4.1 Refinement:** The TSF shall [*overwrite the oldest stored audit records*] and [*no other actions*] if the  
839 audit trail is full.

840 **Assurance Activity:**

841 The following assurance activities are required when storing audit records inside the TOE.

842 *TSS:*

843 The evaluator shall check to ensure that the TSS contains a description of the processing performed when  
844 the capacity of audit records becomes full, which is consistent with the definition of the SFR.

845 *Operational Guidance:*

846 The evaluator shall check to ensure that the operational guidance contains a description of the processing  
847 performed (such as informing the authorized users) when the capacity of audit records becomes full.

848 *Test:*

849 The evaluator shall also perform the following tests:

- 850 1. The evaluator generates auditable events after the capacity of audit records becomes full by  
851 generating auditable events in accordance with the operational guidance.
- 852 2. The evaluator shall check to ensure that the processing defined in the SFR is appropriately  
853 performed to audit records.

### 854 6.3 Class FCO: Communication

855 There are no class FCO requirements.

### 856 6.4 Class FCS: Cryptographic Support

#### 857 6.4.1 FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

858 (for O.COMMS\_PROTECTION)

859 Hierarchical to: No other components.

860 Dependencies: [FCS\_COP.1(b) Cryptographic Operation (for signature generation/ verification)]

861 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

862 **FCS\_CKM.1.1(a) Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment**  
863 in accordance **with [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment**  
864 **Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes]** and  
865 **specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**

#### 866 **Application Note:**

867 *The ST author selects the key generation scheme used for key establishment and device authentication. If*  
868 *multiple schemes are supported, then the ST author should iterate this component to capture this*  
869 *capability. When key generation is used for device authentication, the public key is expected to be*  
870 *associated with an X.509v3 certificate. If the TOE acts as a receiver in the RSA key establishment scheme,*  
871 *the TOE does not need to implement RSA key generation.*

872 *Since the domain parameters to be used are specified by the requirements of the protocol in this PP, it is*  
873 *not expected that the TOE will generate domain parameters, and therefore there is no additional domain*  
874 *parameter validation needed when the TOE complies with the protocols specified in this PP.*

875 *SP 800-56B references (but does not mandate) key generation according to FIPS 186-3. For purposes of*  
876 *compliance in this version of the HCD PP, RSA key pair generation according to FIPS 186-4 is allowed in*  
877 *order for the TOE to claim conformance to SP 800-56B.*

878 *The generated key strength of 2048-bit DSA and rDSA keys need to be equivalent to, or greater than, a*  
879 *symmetric key strength of 112 bits. See NIST Special Publication 800-57, "Recommendation for Key*  
880 *Management" for information about equivalent key strengths.*

#### 881 **Assurance Activity:**

882 TSS:

883 The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A  
884 and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A  
885 and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is  
886 among those sections that the TSF claims to implement.

887 Any TOE-specific extensions, processing that is not included in the documents, or alternative  
888 implementations allowed by the documents that may impact the security requirements the TOE is to  
889 enforce shall be described in the TSS.

890 The TSS may refer to the Key Management Description (KMD), described in Appendix F , that may not be  
891 made available to the public.

892 Test:

893 The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm  
894 Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System  
895 (ECDSA2VS)", and "The 186-4 RSA Validation System (RSA2VS)" as a guide in testing the requirement  
896 above, depending on the selection performed by the ST author. This will require that the evaluator have a  
897 trusted reference implementation of the algorithms that can produce test vectors that are verifiable  
898 during the test.

#### 899 6.4.2 FCS\_CKM.1(b)[DAR] Cryptographic key generation (Symmetric Keys) [Data At Rest]

900 (for O.STORAGE\_ENCRYPTION)

901 Hierarchical to: No other components.

902 Dependencies: [FCS\_COP.1(f) Cryptographic Operation (Key Encryption)]

903 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

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

905 **FCS\_CKM.1.1(b)[DAR] Refinement:** The TSF shall generate **symmetric** cryptographic keys **using a Random Bit**  
906 **Generator as specified in FCS\_RBG\_EXT.1 and specified cryptographic key sizes [256 bit] that meet the**  
907 **following: No Standard.**

908 **Application Note:**

909 *Symmetric keys may be used to generate keys along the key chain.*

910 **Assurance activity:**

911 TSS:

912 The evaluator shall review the TSS to determine that it describes how the functionality described by  
913 FCS\_RBG\_EXT.1 is invoked.

914 KMD:

915 If the TOE is relying on random number generation from a third-party source, the KMD needs to describe  
916 the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs  
917 to include a short description of the vendor's assumption for the amount of entropy seeding the third-



918 party DRBG. The evaluator uses the description of the RBG functionality in FCS\_RBG\_EXT or the KMD to  
919 determine that the key size being requested is identical to the key size and mode to be used for the  
920 encryption/decryption of the user data (FCS\_COP.1(d)).

#### 921 6.4.3 FCS\_CKM.1(b)[DIM] Cryptographic key generation (Symmetric Keys) [Data In Motion]

922 (for O.COMMS\_PROTECTION)

923 Hierarchical to: No other components.

924 Dependencies: [FCS\_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)  
925 FCS\_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)]

926 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

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

928 **FCS\_CKM.1.1(b)[DIM] Refinement:** The TSF shall generate **symmetric** cryptographic keys **using a Random Bit**  
929 **Generator as specified in FCS\_RBG\_EXT.1 and specified cryptographic key sizes [128 bit, 256 bit] that meet**  
930 **the following: No Standard.**

#### 931 **Application Note:**

932 *Symmetric keys may be used to generate keys along the key chain.*

#### 933 **Assurance activity:**

934 *TSS:*

935 The evaluator shall review the TSS to determine that it describes how the functionality described by  
936 FCS\_RBG\_EXT.1 is invoked.

937 *KMD:*

938 If the TOE is relying on random number generation from a third-party source, the KMD needs to describe  
939 the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs  
940 to include a short description of the vendor's assumption for the amount of entropy seeding the third-  
941 party DRBG. The evaluator uses the description of the RBG functionality in FCS\_RBG\_EXT or the KMD to  
942 determine that the key size being requested is identical to the key size and mode to be used for the  
943 encryption/decryption of the user data (FCS\_COP.1(d)).

#### 944 6.4.4 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

945 (for O.COMMS\_PROTECTION, O.STORAGE\_ENCRYPTION)

946 Hierarchical to: No other components.

947 Dependencies: [FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or  
948 FCS\_CKM.1(b) Cryptographic key generation (Symmetric Keys)],

949 FCS\_CKM.4 Cryptographic key destruction

950 **FCS\_CKM\_EXT.4.1** The TSF shall destroy **all plaintext secret and private cryptographic keys and cryptographic**  
951 **critical security parameters** when no longer needed.

#### 952 **Application Note:**

953 *“Cryptographic Critical Security Parameters” are defined in FIPS 140-2 as “security-related information*  
954 *(e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose*  
955 *disclosure or modification can compromise the security of a cryptographic module”.*

956 *Keys, including intermediate keys and key material that are no longer needed are destroyed by using an*  
957 *approved method, FCS\_CKM.4.1. Examples of keys are intermediate keys, submasks, and BEV. There may*  
958 *be instances where keys or key material that are contained in persistent storage are no longer needed and*  
959 *require destruction. Based on their implementation, vendors will explain when certain keys are no longer*  
960 *needed. There are multiple situations in which key material is no longer necessary, for example, a*  
961 *wrapped key may need to be destroyed when a password is changed. However, there are instances when*  
962 *keys are allowed to remain in memory, for example, a device identification key.*

963 **Assurance activity:**

964 TSS:

965 The evaluator shall verify the TSS provides a high level description of what it means for keys and key  
966 material to be no longer needed and when then should be expected to be destroyed.

967 KMD:

968 The evaluator shall verify the Key Management Description (KMD) includes a description of the areas  
969 where keys and key material reside and when the keys and key material are no longer needed.

970 The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material  
971 reside, how the key material is used, how it is determined that keys and key material are no longer  
972 needed, and how the material is destroyed once it is not needed and that the documentation in the KMD  
973 follows FCS\_CKM.4 for the destruction.

974 **6.4.5 FCS\_CKM.4 Cryptographic key destruction**

975 (for O.COMMS\_PROTECTION, O.STORAGE\_ENCRYPTION)

976 Hierarchical to: No other components.

977 Dependencies: [FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or  
978 FCS\_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

979 **FCS\_CKM.4.1 Refinement:** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic  
980 key destruction method [**For volatile memory, the destruction shall be executed by [removal of power to**  
981 **the memory]; For nonvolatile storage, the destruction shall be executed by a [single] overwrite of key data**  
982 **storage location consisting of [a new value of a key of the same size]] that meets the following: [no**  
983 **standard].**

984 **Application Note:**

985 *In the first selection, the ST Author is presented options for destroying disused cryptographic keys based on*  
986 *whether they are in volatile memory or non-volatile memory within the TOE.*

987 *The selection of block erase for non-volatile memory applies only to flash memory.*

988 *Within the selections is the option to overwrite the memory location with a new value of a key. The intent*  
989 *is that a new value of a key (as specified in another SFR within the PP) can be used to “replace” an existing*  
990 *key.*

991 *Several selections allow assignment of a ‘value that does not contain any CSP’. This means that the TOE*  
992 *uses some other specified data not drawn from a source that may contain key material or reveal*  
993 *information about key material, and not being any of the particular values listed as other selection*  
994 *options. The point of the phrase ‘does not contain any CSP’ is to ensure that the overwritten data is*  
995 *carefully selected, and not taken from a general ‘pool’ that might contain current or residual data that*  
996 *itself requires confidentiality protection.*

997 **Assurance activity:**

998 *TSS:*

999 The evaluator shall verify the TSS provides a high level description of how keys and key material are  
1000 destroyed.

1001 If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator  
1002 examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify  
1003 that the pattern does not contain any CSPs.

1004 The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly  
1005 conform to the key destruction requirement.

1006 *KMD:*

1007 The evaluator examines the KMD to ensure it describes how the keys are managed in volatile memory.  
1008 This description includes details of how each identified key is introduced into volatile memory (e.g. by  
1009 derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how  
1010 they are overwritten.

1011 The evaluator shall check to ensure the KMD lists each type of key that is stored in non-volatile memory,  
1012 and identifies the memory type (volatile or non-volatile) where key material is stored.

1013 The KMD identifies and describes the interface(s) that is used to service commands to read/write  
1014 memory. The evaluator examines the interface description for each different media type to ensure that  
1015 the interface supports the selection(s) made by the ST Author.

1016 *Test:*

1017 For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine)  
1018 and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of  
1019 the key that may have been created internally by the TOE during normal cryptographic processing with  
1020 that key.

1021 **Test 1:** Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE  
1022 (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the  
1023 case where the only selection made for the destruction method key was removal of power, then this test  
1024 is unnecessary. The evaluator shall:

- 1025           1. Record the value of the key in the TOE subject to clearing.
- 1026           2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
- 1027           3. Cause the TOE to clear the key.
- 1028           4. Cause the TOE to stop the execution but not exit.
- 1029           5. Cause the TOE to dump the entire memory of the TOE into a binary file.
- 1030           6. Search the content of the binary file created in Step #5 for instances of the known key value from
- 1031                 Step #1.

1032           Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found,

1033           then the test fails.

1034           **Test 2:** Applied to each key held in non-volatile memory and subject to destruction by the TOE, except for

1035           replacing a key using the selection [*a new value of a key of the same size*]. The evaluator shall use special

1036           tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

- 1037           1. Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data
- 1038                 encryption key being deleted would cause data decryption to fail.)
- 1039           2. Cause the TOE to clear the key.
- 1040           3. Have the TOE attempt the functionality that the cleared key would be necessary for. The test
- 1041                 succeeds if step 3 fails.

1042           **Test 3:** Applied to each key held in non-volatile memory and subject to destruction by overwrite by the

1043           TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to

1044           view the key storage location:

- 1045           1. Record the value of the key in the TOE subject to clearing.
- 1046           2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
- 1047           3. Cause the TOE to clear the key.
- 1048           4. Search the non-volatile memory the key was stored in for instances of the known key value from
- 1049                 Step #1. If a copy is found, then the test fails.

1050           **Test 4:** Applied to each key held as non-volatile memory and subject to destruction by overwrite by the

1051           TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to

1052           view the key storage location:

- 1053           1. Record the storage location of the key in the TOE subject to clearing.
- 1054           2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
- 1055           3. Cause the TOE to clear the key.
- 1056           4. Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern
- 1057                 is utilized.

1058 The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is  
1059 not found the test fails.

#### 1060 6.4.6 FCS\_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

1061 (for O.COMMS\_PROTECTION)

1062 Hierarchical to: No other components.

1063 Dependencies: [FCS\_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

1064 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

1065 **FCS\_COP.1.1(a) Refinement:** The TSF shall perform **encryption and decryption** in accordance with a specified  
1066 cryptographic algorithm **AES operating in [CBC]** and cryptographic key sizes **128-bits and 256-bits** that meets  
1067 the following:

- 1068 ▪ **FIPS PUB 197, “Advanced Encryption Standard (AES)”**
- 1069 ▪ **[NIST SP 800-38A]**

#### 1070 **Application Note:**

1071 *For the assignment, the ST author should assign the mode or modes in which AES operates to support the*  
1072 *cryptographic protocols chosen for FTP\_ITC and FTP\_TRP.*

1073 *For the selection, the ST author should choose the standards that describe the modes specified in the*  
1074 *assignment.*

#### 1075 **Assurance Activity:**

1076 *Test:*

1077 The evaluator shall use tests appropriate to the modes selected in the above requirement from "The  
1078 Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", The CMAC Validation System  
1079 (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation  
1080 System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these  
1081 documents are available from <http://csrc.nist.gov/groups/STM/cavp/index.html>) as a guide in testing the  
1082 requirement above. This will require that the evaluator have a reference implementation of the  
1083 algorithms known to be good that can produce test vectors that are verifiable during the test.

#### 1084 6.4.7 FCS\_COP.1(b) Cryptographic Operation (for signature generation/verification)

1085 (for O.UPDATE\_VERIFICATION, O.COMMS\_PROTECTION)

1086 Hierarchical to: No other components.

1087 Dependencies: [FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]

1088 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

1089 **FCS\_COP.1.1(b) Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a **[RSA**  
1090 **Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits]] that meets the following FIPS**  
1091 **PUB 186-4, “Digital Signature Standard”**].

#### 1092 **Application Note:**

1093 *The ST Author should choose the algorithm implemented to perform digital signatures; if more than one*  
1094 *algorithm is available, this requirement (and the corresponding FCS\_CKM.1 requirement) should be*  
1095 *iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate*  
1096 *assignments/selections to specify the parameters that are implemented for that algorithm.*

1097 *For elliptic curve-based schemes, the key size refers to the log2 of the order of the base point.*

1098 **Assurance Activity:**

1099 *Test:*

1100 The evaluator shall use the signature generation and signature verification portions of "The Digital  
1101 Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm  
1102 Validation System" (ECDSA2VS), and "The RSA Validation System" RSA2VS as a guide in testing the  
1103 requirement above. The Validation System used shall comply with the conformance standard identified in  
1104 the ST (i.e., FIPS PUB 186-4). This will require that the evaluator have a reference implementation of the  
1105 algorithms known to be good that can produce test vectors that are verifiable during the test.

1106 **6.4.8 FCS\_COP.1(c)[L1] Cryptographic operation (Hash Algorithm)**

1107 (selected in FPT\_TUD\_EXT.1.3, or with FCS\_SNI\_EXT.1.1)

1108 Hierarchical to: No other components.

1109 Dependencies: No dependencies.

1110 **FCS\_COP.1.1(c)[L1] Refinement:** The TSF shall perform **cryptographic hashing services** in accordance with [SHA-  
1111 **1]** that meet the following: [ISO/IEC 10118-3:2004].

1112 **Application Note (for O.STORAGE\_ENCRYPTION):**

1113 *The hash selection should be consistent with the overall strength of the algorithm used for FCS\_COP.1(d).*  
1114 *(SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The*  
1115 *selection of the standard is made based on the algorithms selected.*

1116 *Vendors are strongly encouraged to implement updated protocols that support the SHA-2 family; until*  
1117 *updated protocols are supported, this PP allows support for SHA-1 implementations in compliance with SP*  
1118 *800-131A.*

1119 **Assurance activity:**

1120 *TSS:*

1121 The evaluator shall check that the association of the hash function with other TSF cryptographic functions  
1122 (for example, the digital signature verification function) is documented in the TSS.

1123 *Operational Guidance:*

1124 The evaluator checks the operational guidance documents to determine that any configuration that is  
1125 required to be done to configure the functionality for the required hash sizes is present.

1126 *Test:*

1127 The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented  
1128 mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the  
1129 length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In  
1130 this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an  
1131 indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

1132 The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and  
1133 used to satisfy the requirements of this PP.

#### 1134 Short Messages Test - Bit-oriented Mode

1135 The evaluators devise an input set consisting of  $m+1$  messages, where  $m$  is the block length of the hash  
1136 algorithm. The length of the messages range sequentially from 0 to  $m$  bits. The message text shall be  
1137 pseudorandomly generated. The evaluators compute the message digest for each of the messages and  
1138 ensure that the correct result is produced when the messages are provided to the TSF.

#### 1139 Short Messages Test - Byte-oriented Mode

1140 The evaluators devise an input set consisting of  $m/8+1$  messages, where  $m$  is the block length of the hash  
1141 algorithm. The length of the messages range sequentially from 0 to  $m/8$  bytes, with each message being  
1142 an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators  
1143 compute the message digest for each of the messages and ensure that the correct result is produced  
1144 when the messages are provided to the TSF.

#### 1145 Selected Long Messages Test - Bit-oriented Mode

1146 The evaluators devise an input set consisting of  $m$  messages, where  $m$  is the block length of the hash  
1147 algorithm. For SHA-256, the length of the  $i$ -th message is  $512 + 99*i$ , where  $1 \leq i \leq m$ . For SHA-512, the  
1148 length of the  $i$ -th message is  $1024 + 99*i$ , where  $1 \leq i \leq m$ . The message text shall be pseudorandomly  
1149 generated. The evaluators compute the message digest for each of the messages and ensure that the  
1150 correct result is produced when the messages are provided to the TSF.

#### 1151 Selected Long Messages Test - Byte-oriented Mode

1152 The evaluators devise an input set consisting of  $m/8$  messages, where  $m$  is the block length of the hash  
1153 algorithm. For SHA-256, the length of the  $i$ -th message is  $512 + 8*99*i$ , where  $1 \leq i \leq m/8$ . For SHA-512,  
1154 the length of the  $i$ -th message is  $1024 + 8*99*i$ , where  $1 \leq i \leq m/8$ . The message text shall be  
1155 pseudorandomly generated. The evaluators compute the message digest for each of the messages and  
1156 ensure that the correct result is produced when the messages are provided to the TSF.

#### 1157 Pseudorandomly Generated Messages Test

1158 This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is  $n$  bits  
1159 long, where  $n$  is the length of the message digest produced by the hash function to be tested. The  
1160 evaluators then formulate a set of 100 messages and associated digests by following the algorithm  
1161 provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure  
1162 that the correct result is produced when the messages are provided to the TSF.



1163 **6.4.9 FCS\_COP.1(c) [L2] Cryptographic operation (Hash Algorithm)**

1164 (selected in FPT\_TUD\_EXT.1.3, or with FCS\_SNI\_EXT.1.1)

1165 Hierarchical to: No other components.

1166 Dependencies: No dependencies.

1167 **FCS\_COP.1.1(c)[L2] Refinement:** The TSF shall perform **cryptographic hashing services** in accordance with [**SHA-**  
1168 **256, SHA-384, SHA-512**] that meet the following: [**ISO/IEC 10118-3:2004**].

1169 ***Application Note (for O.STORAGE\_ENCRYPTION):***

1170 *The hash selection should be consistent with the overall strength of the algorithm used for FCS\_COP.1(d).*  
1171 *(SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The*  
1172 *selection of the standard is made based on the algorithms selected.*

1173 *Vendors are strongly encouraged to implement updated protocols that support the SHA-2 family; until*  
1174 *updated protocols are supported, this PP allows support for SHA-1 implementations in compliance with SP*  
1175 *800-131A.*

1176 **Assurance activity:**

1177 **TSS:**

1178 The evaluator shall check that the association of the hash function with other TSF cryptographic functions  
1179 (for example, the digital signature verification function) is documented in the TSS.

1180 ***Operational Guidance:***

1181 The evaluator checks the operational guidance documents to determine that any configuration that is  
1182 required to be done to configure the functionality for the required hash sizes is present.

1183 ***Test:***

1184 The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented  
1185 mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the  
1186 length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In  
1187 this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an  
1188 indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

1189 The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and  
1190 used to satisfy the requirements of this PP.

1191 **Short Messages Test - Bit-oriented Mode**

1192 The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash  
1193 algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be  
1194 pseudorandomly generated. The evaluators compute the message digest for each of the messages and  
1195 ensure that the correct result is produced when the messages are provided to the TSF.

1196 **Short Messages Test - Byte-oriented Mode**



1197 The evaluators devise an input set consisting of  $m/8+1$  messages, where  $m$  is the block length of the hash  
1198 algorithm. The length of the messages range sequentially from 0 to  $m/8$  bytes, with each message being  
1199 an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators  
1200 compute the message digest for each of the messages and ensure that the correct result is produced  
1201 when the messages are provided to the TSF.

1202 Selected Long Messages Test - Bit-oriented Mode

1203 The evaluators devise an input set consisting of  $m$  messages, where  $m$  is the block length of the hash  
1204 algorithm. For SHA-256, the length of the  $i$ -th message is  $512 + 99*i$ , where  $1 \leq i \leq m$ . For SHA-512, the  
1205 length of the  $i$ -th message is  $1024 + 99*i$ , where  $1 \leq i \leq m$ . The message text shall be pseudorandomly  
1206 generated. The evaluators compute the message digest for each of the messages and ensure that the  
1207 correct result is produced when the messages are provided to the TSF.

1208 Selected Long Messages Test - Byte-oriented Mode

1209 The evaluators devise an input set consisting of  $m/8$  messages, where  $m$  is the block length of the hash  
1210 algorithm. For SHA-256, the length of the  $i$ -th message is  $512 + 8*99*i$ , where  $1 \leq i \leq m/8$ . For SHA-512,  
1211 the length of the  $i$ -th message is  $1024 + 8*99*i$ , where  $1 \leq i \leq m/8$ . The message text shall be  
1212 pseudorandomly generated. The evaluators compute the message digest for each of the messages and  
1213 ensure that the correct result is produced when the messages are provided to the TSF.

1214 Pseudorandomly Generated Messages Test

1215 This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is  $n$  bits  
1216 long, where  $n$  is the length of the message digest produced by the hash function to be tested. The  
1217 evaluators then formulate a set of 100 messages and associated digests by following the algorithm  
1218 provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure  
1219 that the correct result is produced when the messages are provided to the TSF.

1220 **6.4.10 FCS\_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)**

1221 (for O. STORAGE\_ENCRYPTION)

1222 Hierarchical to: No other components.

1223 Dependencies: [FCS\_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

1224 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

1225 **FCS\_COP.1.1(d)** The TSF shall perform **data encryption and decryption** in accordance with a specified  
1226 cryptographic algorithm **AES used in [CBC] mode and cryptographic key sizes [256 bits] that meet the**  
1227 **following: AES as specified in ISO/IEC 18033-3, [CBC as specified in ISO/IEC 10116].**

1228 **Application Note:**

1229 *This PP allows for software encryption or hardware encryption.*

1230 *If XTS Mode is selected, a cryptographic key of 256-bit or of 512-bit is allowed as specified in IEEE 1619.*  
1231 *XTS-AES key is divided into two AES keys of equal size - for example, AES-128 is used as the underlying*  
1232 *algorithm, when 256-bit key and XTS mode are selected. AES-256 is used when a 512-bit key and XTS*  
1233 *mode are selected.*

1234 *The intent of this requirement is to specify the approved AES modes that the ST Author may select for AES*  
1235 *encryption of the appropriate information on the Field-Replaceable Nonvolatile Storage Device. For the*  
1236 *first selection, the ST author should indicate the mode or modes supported by the TOE implementation.*  
1237 *The second selection indicates the key size to be used, which is identical to that specified for*  
1238 *FCS\_CKM.1(b). The third selection must agree with the mode or modes chosen in the first selection. If*  
1239 *multiple modes are supported, it may be clearer in the ST if this component was iterated.*

1240 **Assurance activity:**

1241 TSS:

1242 The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode  
1243 used for encryption.

1244 *Operational Guidance:*

1245 If multiple encryption modes are supported, the evaluator examines the guidance documentation to  
1246 determine that the method of choosing a specific mode/key size by the end user is described.

1247 **Test:**

1248 The following tests are conditional based upon the selections made in the SFR.

1249 AES-CBC Tests

1250 AES-CBC Known Answer Tests

1251 There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV  
1252 values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly  
1253 or by supplying the inputs to the implementer and receiving the results in response. To determine  
1254 correctness, the evaluator shall compare the resulting values to those obtained by submitting the same  
1255 inputs to a known good implementation.

1256 **KAT-1.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values  
1257 and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key  
1258 value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros  
1259 key, and the other five shall be encrypted with a 256-bit all-zeros key.

1260 To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt,  
1261 using 10 ciphertext values as input and AES-CBC decryption.

1262 **KAT-2.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and  
1263 obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given  
1264 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  
1265 keys.

1266 To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt,  
1267 using an all-zero ciphertext value as input and AES-CBC decryption.

1268 **KAT-3.** To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values  
1269 described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext

1270 using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the  
1271 second set shall have 256 256-bit keys. Key  $i$  in each set shall have the leftmost  $i$  bits be ones and the  
1272 rightmost  $N-i$  bits be zeros, for  $i$  in  $[1,N]$ .

1273 To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext  
1274 value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the  
1275 given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have  
1276 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit  
1277 key/ciphertext pairs. Key  $i$  in each set shall have the leftmost  $i$  bits be ones and the rightmost  $N-i$  bits be  
1278 zeros, for  $i$  in  $[1,N]$ . The ciphertext value in each pair shall be the value that results in an all-zeros plaintext  
1279 when decrypted with its corresponding key.

1280 **KAT-4.** To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext  
1281 values described below and obtain the two ciphertext values that result from AES-CBC encryption of the  
1282 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  
1283 all zeros with an IV of all zeros, respectively. Plaintext value  $i$  in each set shall have the leftmost  $i$  bits be  
1284 ones and the rightmost  $128-i$  bits be zeros, for  $i$  in  $[1,128]$ .

1285 To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt,  
1286 using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC  
1287 decryption.

#### 1288 AES-CBC Multi-Block Message Test

1289 The evaluator shall test the encrypt functionality by encrypting an  $i$ -block message where  $1 < i \leq 10$ . The  
1290 evaluator shall choose a key, an IV and plaintext message of length  $i$  blocks and encrypt the message,  
1291 using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of  
1292 encrypting the same plaintext message with the same key and IV using a known good implementation.

1293 The evaluator shall also test the decrypt functionality for each mode by decrypting an  $i$ -block message  
1294 where  $1 < i \leq 10$ . The evaluator shall choose a key, an IV and a ciphertext message of length  $i$  blocks and  
1295 decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be  
1296 compared to the result of decrypting the same ciphertext message with the same key and IV using a  
1297 known good implementation.

#### 1298 AES-CBC Monte Carlo Tests

1299 The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of  
1300 these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit  
1301 blocks. For each 3-tuple, 1000 iterations shall be run as follows:

1302 # Input: PT, IV, Key

1303 for  $i = 1$  to 1000:

1304     if  $i == 1$ :

1305         CT[1] = AES-CBC-Encrypt(Key, IV, PT)

1306         PT = IV

1307            else:  
1308                    CT[i] = AES-CBC-Encrypt(Key, PT)  
1309                    PT = CT[i-1]

1310            The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall  
1311            be compared to the result of running 1000 iterations with the same values using a known good  
1312            implementation.  
1313            The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT  
1314            and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

#### 1315    6.4.11 FCS\_COP.1(f) Cryptographic operation (Key Encryption)

1316            (selected from FCS\_KYC\_EXT.1.1)  
1317            Hierarchical to:    No other components.  
1318            Dependencies:    [FCS\_CKM.1(b) Cryptographic key generation (Symmetric Keys)]  
1319                                FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

1320    **FCS\_COP.1.1(f) Refinement:** The TSF shall perform **key encryption and decryption** in accordance with a  
1321    specified cryptographic algorithm **AES used in [[CBC] mode]** and cryptographic key sizes **[256 bits]** that meet  
1322    the following: **AES as specified in ISO /IEC 18033-3, [CBC as specified in ISO/IEC 10116].**

#### 1323    **Application Note:**

1324            *This requirement is used in the body of the ST if the ST Author chooses to use AES encryption/decryption*  
1325            *for protecting the keys as part of the key chaining approach that is specified in FCS\_KYC\_EXT.1.*

#### 1326    **Assurance activity:**

1327            TSS:  
1328                    The evaluator shall verify the TSS includes a description of the key encryption function(s) and shall verify  
1329                    the key encryption uses an approved algorithm according to the appropriate specification.

#### 1330            KMD:

1331                    The evaluator shall review the KMD to ensure that all keys are encrypted using the approved method and  
1332                    a description of when the key encryption occurs is provided.

#### 1333            Test:

1334                    The evaluator shall use tests in FCS\_COP.1(d) to verify encryption.

#### 1335    6.4.12 FCS\_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

1336            (selected with FCS\_IPSEC\_EXT.1.4)  
1337            Hierarchical to:    No other components.  
1338            Dependencies:    [FDP\_ITC.1 Import of user data without security attributes, or  
1339                                FDP\_ITC.2 Import of user data with security attributes, or  
1340                                FCS\_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

1341 FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

1342 **FCS\_COP.1.1(g) Refinement:** The TSF shall perform **keyed-hash message authentication** in accordance with a  
1343 specified cryptographic algorithm **Hash-[SHA-256, SHA-384, SHA-512]**, key size [**64 (when using SHA-256),**  
1344 **128 (when using SHA-384 or SHA-512)**], and message digest sizes [**256, 384, 512**] bits that meet the  
1345 following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure**  
1346 **Hash Standard."**

1347 **Assurance Activity:**

1348 *Test:*

1349 The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System  
1350 (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a  
1351 reference implementation of the algorithms known to be good that can produce test vectors that are  
1352 verifiable during the test.

1353 **6.4.13 FCS\_HTTPS\_EXT.1 Extended: HTTPS selected**

1354 (selected in FTP\_TRP.1.1)

1355 Hierarchical to: No other components.

1356 Dependencies: FCS\_TLS\_EXT.1 Extended: TLS selected.

1357 **FCS\_HTTPS\_EXT.1.1** The TSF shall implement the HTTPS protocol that complies with RFC 2818.

1358 **Application Note:**

1359 *The ST author must provide enough detail to determine how the implementation is complying with the*  
1360 *standard(s) identified; this can be done either by adding elements to this component, or by additional*  
1361 *detail in the TSS.*

1362 **FCS\_HTTPS\_EXT.1.2** The TSF shall implement HTTPS using TLS as specified in FCS\_TLS\_EXT.1.

1363 **Assurance Activity:**

1364 *TSS:*

1365 The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an  
1366 administrative session, focusing on any client authentication required by the TLS protocol vs. security  
1367 administrator authentication which may be done at a different level of the processing stack.

1368 *Test:*

1369 Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS  
1370 tests are done at the TLS protocol level.

1371 **6.4.14 FCS\_IPSEC\_EXT.1 Extended: IPsec selected**

1372 (selected in FTP\_ITC.1.1, FTP\_TRP.1.1)

1373 Hierarchical to: No other components.

1374 Dependencies: FIA\_PSK\_EXT.1 Extended: Pre-Shared Key Composition

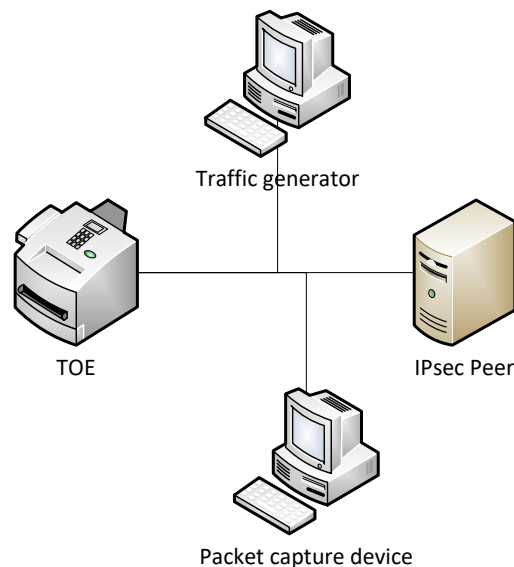
1375 FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

- 1376 FCS\_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
- 1377 FCS\_COP.1(b) Cryptographic Operation (for signature generation/verification)
- 1378 FCS\_COP.1(c)[L2] Cryptographic Operation (Hash Algorithm)
- 1379 FCS\_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
- 1380 FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

**Application Note:**

1382 *In order to show that the TSF implements the RFCs in accordance with the requirements of this PP, the*  
1383 *evaluator shall perform the assurance activities listed below.*

1384 *The TOE is required to use the IPsec protocol to establish connections used to communicate with an IPsec*  
1385 *Peer.*



1386  
1387 *The evaluators shall minimally create a test environment equivalent to the test environment illustrated*  
1388 *above. It is expected that the traffic generator is used to construct network packets and will provide the*  
1389 *evaluator with the ability manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The*  
1390 *evaluators must provide justification for any differences in the test environment.*

1391 **FCS\_IPSEC\_EXT.1.1** The TSF shall implement the IPsec architecture as specified in RFC 4301.

**Application Note:**

1393 *RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy*  
1394 *Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g.,*  
1395 *encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the*  
1396 *packet). The SPD can be implemented in various ways, including router access control lists, firewall*  
1397 *rulesets, a “traditional” SPD, etc. Regardless of the implementation details, there is a notion of a “rule”*  
1398 *that a packet is “matched” against and a resulting action that take place.*

1399 *While there must be a means to order the rules, a general approach to ordering is not mandated, as long*  
1400 *as the SPD can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one*  
1401 *for each network interface), but this is not required.*

1402 **Assurance Activity:**

1403 *TSS:*

1404 The evaluator shall examine the TSS and determine that it describes what takes place when a packet is  
1405 processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is  
1406 implemented and the rules for processing both inbound and outbound packets in terms of the IPsec  
1407 policy. The TSS describes the rules that are available and the resulting actions available after matching a  
1408 rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no  
1409 encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in  
1410 RFC 4301.

1411 As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator  
1412 shall determine that the description in the TSS is sufficient to determine which rules will be applied given  
1413 the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges,  
1414 conditional rules, etc., the evaluator shall determine that the description of rule processing (for both  
1415 inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the  
1416 case where two different rules may apply. This description shall cover both the initial packets (that is, no  
1417 SA is established on the interface or for that particular packet) as well as packets that are part of an  
1418 established SA.

1419 *Operational Guidance:*

1420 The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to  
1421 construct entries into the SPD that specify a rule for processing a packet. The description includes all three  
1422 cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without  
1423 being encrypted. The evaluator shall determine that the description in the guidance documentation is  
1424 consistent with the description in the TSS, and that the level of detail in the guidance documentation is  
1425 sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a  
1426 discussion of how ordering of rules impacts the processing of an IP packet.

1427 *Test:*

1428 The evaluator uses the guidance documentation to configure the TOE to carry out the following tests:

1429 a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting  
1430 a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction  
1431 of the rule shall be different such that the evaluator can generate a packet and send packets to the  
1432 gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP  
1433 ports) in the packet header. The evaluator performs both positive and negative test cases for each type of  
1434 rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator  
1435 observes via the audit trail, and packet captures that the TOE exhibited the expected behavior:  
1436 appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec  
1437 implementation.



1438 b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing.  
1439 As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These  
1440 scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the  
1441 TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and  
1442 conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that  
1443 belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each  
1444 scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance  
1445 documentation.

1446 **FCS\_IPSEC\_EXT.1.2** The TSF shall implement [**transport mode**].

1447 **Assurance Activity:**

1448 *TSS:*

1449 The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel  
1450 mode and/or transport mode (as selected).

1451 *Operational Guidance:*

1452 The evaluator shall confirm that the operational guidance contains instructions on how to configure the  
1453 connection in each mode selected.

1454 *Test:*

1455 The evaluator shall perform the following test(s) based on the selections chosen:

1456 1. (conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the  
1457 TOE to operate in tunnel mode and also configures an IPsec Peer to operate in tunnel mode. The  
1458 evaluator configures the TOE and the IPsec Peer to use any of the allowable cryptographic algorithms,  
1459 authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then  
1460 initiate a connection from the client to connect to the IPsec Peer. The evaluator observes (for example, in  
1461 the audit trail and the captured packets) that a successful connection was established using the tunnel  
1462 mode.

1463 2. (conditional): If transport mode is selected, the evaluator uses the operational guidance to configure  
1464 the TOE to operate in transport mode and also configures an IPsec Peer to operate in transport mode. The  
1465 evaluator configures the TOE and the IPsec Peer to use any of the allowed cryptographic algorithms,  
1466 authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a  
1467 connection from the TOE to connect to the IPsec Peer. The evaluator observes (for example, in the audit  
1468 trail and the captured packets) that a successful connection was established using the transport mode.

1469 **FCS\_IPSEC\_EXT.1.3** The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise  
1470 unmatched, and discards it.

1471 **Assurance Activity:**

1472 *TSS:*



1473 The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is  
1474 processed against the SPD and that if no “rules” are found to match, that a final rule exists, either  
1475 implicitly or explicitly, that causes the network packet to be discarded.

1476 *Operational Guidance:*

1477 The evaluator checks that the operational guidance provides instructions on how to construct the SPD and  
1478 uses the guidance to configure the TOE for the following tests.

1479 *Test:*

1480 The evaluator shall perform the following test:

1481 The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD,  
1482 BYPASS, and PROTECT network packets. The evaluator may use the SPD that was created for verification  
1483 of FCS\_IPSEC\_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and  
1484 send that packet. The evaluator should observe that the network packet is passed to the proper  
1485 destination interface with no modification. The evaluator shall then modify a field in the packet header;  
1486 such that it no longer matches the evaluator-created entries (there may be a “TOE created” final entry  
1487 that discards packets that do not match any previous entries). The evaluator sends the packet, and  
1488 observes that the packet was not permitted to flow to any of the TOE’s interfaces.

1489 **FCS\_IPSEC\_EXT.1.4** The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [*the*  
1490 *cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm*  
1491 *(SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-*  
1492 *based HMAC*].

1493 **Assurance Activity:**

1494 *TSS:*

1495 The evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along  
1496 with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator  
1497 ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS\_COP.1(g)  
1498 Cryptographic Operations (for keyed-hash message authentication).

1499 *Operational Guidance:*

1500 The evaluator checks the operational guidance to ensure it provides instructions on how to configure the  
1501 TOE to use the algorithms selected by the ST author.

1502 *Test:*

1503 The evaluator shall also perform the following tests:

1504 The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to  
1505 using each of the selected algorithms, and attempt to establish a connection using ESP. The connection  
1506 should be successfully established for each algorithm.

1507 **FCS\_IPSEC\_EXT.1.5** The TSF shall implement the protocol: [*IKEv1, using Main Mode for Phase 1 exchanges, as*  
1508 *defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [RFC 4868*  
1509 *for hash functions];].*

1510 **Application Note:**

1511 *Either IKEv1 or IKEv2 support must be provided, although conformant TOEs can provide both; the first*  
1512 *selection is used to make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE*  
1513 *implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC*  
1514 *4304 identifies support for extended sequence numbers, which compliant TOEs can specify using the*  
1515 *second selection. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these*  
1516 *functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used.*

1517 **Assurance Activity:**

1518 *TSS:*

1519 The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

1520 *Operational Guidance:*

1521 The evaluator shall check the operational guidance to ensure it instructs the administrator how to  
1522 configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to  
1523 perform NAT traversal for the following test if IKEv2 is selected.

1524 *Test:*

1525 (conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT  
1526 traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an  
1527 IPsec connection and determine that the NAT is successfully traversed.

1528 **FCS\_IPSEC\_EXT.1.6** The TSF shall ensure the encrypted payload in the [*IKEv1*] protocol uses the cryptographic  
1529 algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [*no other algorithm*].

1530 **Assurance Activity:**

1531 *TSS:*

1532 The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2  
1533 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the  
1534 selection of the requirement, those are included in the TSS discussion.

1535 *Operational Guidance:*

1536 The evaluator ensures that the operational guidance describes the configuration of the mandated  
1537 algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to  
1538 configure the TOE to perform the following test for each ciphersuite selected.

1539 *Test:*

1540 The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2  
1541 payload and establish a connection with a peer device, which is configured to only accept the payload

1542 encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the  
1543 negotiation.

1544 **FCS\_IPSEC\_EXT.1.7** The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

1545 **Assurance Activity:**

1546 *TSS:*

1547 The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by  
1548 the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode  
1549 is used. It may be that this is a configurable option.

1550 *Operational Guidance:*

1551 If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the  
1552 operational guidance to ensure that instructions for this configuration are contained within that guidance.

1553 *Test:*

1554 The evaluator shall also perform the following test:

1555 (conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt  
1556 to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail.  
1557 The evaluator should then show that main mode exchanges are supported. This test is not applicable if  
1558 IKEv1 is not selected above in the FCS\_IPSEC\_EXT.1.5 protocol selection.

1559 **FCS\_IPSEC\_EXT.1.8** The TSF shall ensure that [*IKEv1 SA lifetimes can be established based on [length of time,*  
1560 *where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]*].

1561 **Application Note:**

1562 *The ST Author is afforded a selection based on the version of IKE in their implementation. If the lifetime*  
1563 *limitations are configurable, then the evaluator verifies that the appropriate instructions for configuring*  
1564 *these values are included in the operational guidance.*

1565 *As far as SA lifetimes are concerned, the TOE can limit the lifetime based on the number of bytes*  
1566 *transmitted, or the number of packets transmitted. Either packet-based or volume-based SA lifetimes are*  
1567 *acceptable; the ST author makes the appropriate selection to indicate which type of lifetime limits are*  
1568 *supported.*

1569 **Assurance Activity:**

1570 *Operational Guidance:*

1571 The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing  
1572 so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that  
1573 the values allow for Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently there are no  
1574 values mandated for the number of packets or number of bytes, the evaluator just ensures that this can  
1575 be configured if selected in the requirement.

1576 When testing this functionality, the evaluator needs to ensure that both sides are configured  
1577 appropriately. From the RFC “A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were  
1578 negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and  
1579 rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter  
1580 lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime  
1581 policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant  
1582 SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered.”

1583 *Test:*

1584 Each of the following tests shall be performed for each version of IKE selected in the FCS\_IPSEC\_EXT.1.5  
1585 protocol selection:

- 1586 1. (Conditional): The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes)  
1587 allowed following the operational guidance. The evaluator shall establish an SA and determine that once  
1588 the allowed # of packets (or bytes) through this SA is exceeded, the connection is renegotiated.
- 1589 2. (Conditional): The evaluator shall construct a test where a Phase 1 SA is established and attempted to  
1590 be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is  
1591 closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a  
1592 specific way, the evaluator shall implement tests demonstrating that the configuration capability of the  
1593 TOE works as documented in the operational guidance.
- 1594 3. (Conditional): The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the  
1595 lifetime will be 8 hours instead of 24.

1596 **FCS\_IPSEC\_EXT.1.9** The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and  
1597 **[[DH groups 1 and 2]].**

1598 ***Application Note:***

1599 *The above requires that the TOE support DH Group 14. If other groups are supported, then those should*  
1600 *be selected (for groups 24, 19, 20, and 5) or specified in the assignment above; otherwise “no other DH*  
1601 *groups” should be selected. This applies to IKEv1/IKEv2 exchanges.*

1602 **Assurance Activity:**

1603 *TSS:*

1604 The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being  
1605 supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the  
1606 TSS describes how a particular DH group is specified/negotiated with a peer.

1607 *Test:*

1608 The evaluator shall also perform the following test (this test may be combined with other tests for this  
1609 component, for instance, the tests associated with FCS\_IPSEC\_EXT.1.1):

1610 For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully  
1611 completed using that particular DH group.

1612 **FCS\_IPSEC\_EXT.1.10** The TSF shall ensure that all IKE protocols perform Peer Authentication using the [RSA]  
1613 algorithm and Pre-shared Keys.

1614 **Application Note:**

1615 *The selected algorithm should correspond to an appropriate selection for FCS\_COP.1(b). If IPsec is*  
1616 *included in the TOE, the ST author also includes FIA\_PSK\_EXT from Appendix D.2.6.*

1617 **Assurance Activity:**

1618 TSS:

1619 The evaluator shall check that the TSS contains a description of the IKE peer authentication process used  
1620 by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in  
1621 the requirement.

1622 Test:

1623 The evaluator shall also perform the following test:

1624 For each supported signature algorithm, the evaluator shall test that peer authentication using that  
1625 algorithm can be successfully achieved and results in the successful establishment of a connection.

1626 **6.4.15 FCS\_KYC\_EXT.1 Extended: Key Chaining**

1627 (for O.STORAGE\_ENCRYPTION)

1628 Hierarchical to: No other components.

1629 Dependencies: [FCS\_COP.1(e) Cryptographic operation (Key Wrapping),  
1630 FCS\_SMC\_EXT.1 Extended: Submask Combining,  
1631 FCS\_COP.1(f) Cryptographic operation (Key Encryption),  
1632 FCS\_KDF\_EXT.1 Cryptographic Operation (Key Derivation), and/or  
1633 FCS\_COP.1(i) Cryptographic operation (Key Transport)]

1634 **Application Note:**

1635 *This SFR forms a keychain that terminates either with a DEK or a BEV to unlock a self-encrypting drive. If*  
1636 *passwords are not used, it can be a keychain of one, with no intermediate keys forming the DEK or BEV,*  
1637 *provided that key is protected. For example, if the DEK for an SED is not stored on the SED and is released*  
1638 *on power-up, a keychain of one is allowed.*

1639 **FCS\_KYC\_EXT.1.1** The TSF shall maintain a key chain of: [*intermediate keys originating from one or more*  
1640 *submask(s) to the BEV or DEK using the following method(s): [key encryption as specified in FCS\_COP.1(f)]*]  
1641 while maintaining an effective strength of [256 bits].

1642 **Application Note:**

1643 *Key Chaining is the method of using multiple layers of encryption keys to ultimately secure the BEV (Border*  
1644 *Encryption Value). The number of intermediate keys will vary – from one (e.g., taking the conditioned*  
1645 *password authorization factor and directly using it as the BEV) to many. This applies to all keys that*

1646 *contribute to the ultimate wrapping or derivation of the BEV; including those in areas of protected storage*  
1647 *(e.g. TPM stored keys, comparison values).*

1648 *Multiple key chains to the BEV are allowed, as long as all chains meet the key chain requirement.*

1649 *Once the ST Author has selected a method to create the chain (either by unwrapping or encrypting keys),*  
1650 *they pull the appropriate requirement out of this appendix. It is allowable for an implementation to use for*  
1651 *any or all methods.*

1652 *The method the TOE uses to chain keys and manage/protect them is described in the Key Management*  
1653 *Description; see Key Management Description for more information.*

1654 **Assurance activity:**

1655 *TSS:*

1656 The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV  
1657 outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for  
1658 products that support AES-256.

1659 *KMD:*

1660 The evaluator shall examine the KMD to ensure that it describes a high level description of the key  
1661 hierarchy for all accepted BEVs. The evaluator shall examine the KMD to ensure it describes the key chain  
1662 in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using  
1663 key wrap, submask combining, or key encryption.

1664 The evaluator shall examine the KMD to ensure that it describes how the key chain process functions,  
1665 such that it does not expose any material that might compromise any key in the chain. (e.g. using a key  
1666 directly as a compare value against a TPM) This description must include a diagram illustrating the key  
1667 hierarchy implemented and detail where all keys and keying material is stored or what it is derived from.  
1668 The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken  
1669 without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is  
1670 maintained throughout the Key Chain.

1671 The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

#### 1672 **6.4.16 FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)**

1673 (for O.STORAGE\_ENCRYPTION and O.COMMS\_PROTECTION)

1674 Hierarchical to: No other components.

1675 Dependencies: No dependencies.

1676 **FCS\_RBG\_EXT.1.1:** The TSF shall perform all deterministic random bit generation services in accordance with  
1677 **[NIST SP 800-90A]** using **[Hash\_DRBG (refinement: SHA-256)]**.

1678 **FCS\_RBG\_EXT.1.2** The deterministic RBG shall be seeded by at least one entropy source that accumulates  
1679 entropy from **[[one (1)] hardware-based noise source(s)]** with a minimum of **[256 bits]** of entropy at least  
1680 equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table  
1681 for Hash Functions”, of the keys and hashes that it will generate.

1682 **Application Note:**

1683 *ISO/IEC 18031:2011 contains different methods of generating random numbers; each of these, in turn,*  
1684 *depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the*  
1685 *function used and include the specific underlying cryptographic primitives used in the requirement. While*  
1686 *any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for*  
1687 *Hash\_DRBG or HMAC\_DRBG, only AES-based implementations for CTR\_DRBG are allowed. Table C.2 in*  
1688 *ISO/IEC 18031:2011 provides an identification of Security strengths, Entropy and Seed length requirements*  
1689 *for the AES-128 and 256 Block Cipher.*

1690 *The CTR\_DRBG in ISO/IEC 18031:2011 requires using derivation function, whereas NIST SP 800-90A does*  
1691 *not. Either model is acceptable. In the first selection in FCS\_RBG\_EXT.1.1, the ST Author chooses the*  
1692 *standard with which they are compliant.*

1693 *The first selection in FCS\_RBG\_EXT.1.2 the ST author fills in how many entropy sources are used for each*  
1694 *type of entropy source they employ. It should be noted that a combination of hardware and software*  
1695 *based noise sources is acceptable.*

1696 *It should be noted that the entropy source is considered to be a part of the RBG and if the RBG is included*  
1697 *in the TOE, the developer is required to provide the entropy description outlined in Appendix E. The*  
1698 *documentation \*and tests\* required in the Evaluation Activity for this element necessarily cover each*  
1699 *source indicated in FCS\_RBG\_EXT.1.2.*

1700 **Assurance activity:**

1701 **TSS:**

1702 For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement  
1703 about the expected amount of entropy received from such a source, and a full description of the  
1704 processing of the output of the third-party source. The evaluator shall verify that this statement is  
1705 consistent with the selection made in FCS\_RBG\_EXT.1.2 for the seeding of the DRBG. If the ST specifies  
1706 more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each  
1707 DRBG mechanism.

1708 **Entropy Description:**

1709 The evaluator shall ensure the Entropy Description provides all of the required information as described in  
1710 Appendix E. The evaluator assesses the information provided and ensures the TOE is providing sufficient  
1711 entropy when it is generating a Random Bit String.

1712 **Operational Guidance:**

1713 The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to  
1714 use the selected DRBG mechanism(s), if necessary.

1715 **Test:**

1716 The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable by the TOE,  
1717 the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions  
1718 in the operational guidance for configuration of the RBG are valid.



1719 If the RBG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the  
1720 first block of random bits (3) generate a second block of random bits (4) unstantiate. The evaluator  
1721 verifies that the second block of random bits is the expected value. The evaluator shall generate eight  
1722 input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and  
1723 personalization string for the instantiate operation. The next two are additional input and entropy input  
1724 for the first call to generate. The final two are additional input and entropy input for the second call to  
1725 generate. These values are randomly generated. “Generate one block of random bits” means to generate  
1726 random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-  
1727 90A).

1728 If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the  
1729 first block of random bits (3) reseed, (4) generate a second block of random bits (5) unstantiate. The  
1730 evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate  
1731 eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and  
1732 personalization string for the instantiate operation. The fifth value is additional input to the first call to  
1733 generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final  
1734 value is additional input to the second generate call.

1735 The following paragraphs contain more information on some of the input values to be generated/selected  
1736 by the evaluator.

1737 Entropy input: the length of the entropy input value must equal the seed length.

1738 Nonce: If a nonce is supported (CTR\_DRBG with no Derivation Function does not use a nonce), the nonce  
1739 bit length is one-half the seed length.

1740 Personalization string: The length of the personalization string must be  $\leq$  seed length. If the  
1741 implementation only supports one personalization string length, then the same length can be used for  
1742 both values. If more than one string length is support, the evaluator shall use personalization strings of  
1743 two different lengths. If the implementation does not use a personalization string, no value needs to be  
1744 supplied.

1745 Additional input: the additional input bit lengths have the same defaults and restrictions as the  
1746 personalization string lengths.

#### 1747 6.4.17 FCS\_TLS\_EXT.1 Extended: TLS selected

1748 (selected in FTP\_TRP.1.1)

1749 Hierarchical to: No other components.

1750 Dependencies: FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

1751 FCS\_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

1752 FCS\_COP.1(b) Cryptographic Operation (for signature generation/verification)

1753 FCS\_COP.1(c) Cryptographic Operation (Hash Algorithm)

1754 FCS\_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

1755 FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

1756 **FCS\_TLS\_EXT.1.1** The TSF shall implement one or more of the following protocols [**TLS 1.2 (RFC 5246)**]  
1757 supporting the following ciphersuites:



1758

1759 [TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
1760 TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
1761 TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
1762 TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
1763 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
1764 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384  
1765 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
1766 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384].

1767 **Application Note:**

1768 *The ST author must make the appropriate selections and assignments to reflect the TLS implementation.*  
1769 *The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author*  
1770 *should select the ciphersuites that are supported. If administrative steps need to be taken so that the*  
1771 *suites negotiated by the implementation are limited to those in this requirement, the appropriate*  
1772 *instructions need to be contained in the guidance called for by AGD\_OPE.*  
1773 *The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. The TLS*  
1774 *requirement may be changed in the next version of the HCD PP to comply with CNSSP 15 and NIST SP 800-*  
1775 *131A.*

1776 **Assurance Activity:**

1777 TSS:

1778 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that  
1779 the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites  
1780 specified are identical to those listed for this component. The evaluator shall also check the operational  
1781 guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the  
1782 description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be  
1783 restricted to meet the requirements).

1784 *Test:*

1785 The evaluator shall also perform the following test:

- 1786 1. The evaluator shall establish a TLS connection using each of the ciphersuites specified by the  
1787 requirement. This connection may be established as part of the establishment of a higher-level  
1788 protocol, e.g., as part of a HTTPS session. It is sufficient to observe the successful negotiation of a  
1789 ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of  
1790 the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the  
1791 cryptographic algorithm is 128-bit AES and not 256-bit AES).
- 1792 2. The evaluator shall setup a man-in-the-middle tool between the TOE and the TLS Peer and shall  
1793 perform the following modifications to the traffic:

- 1794 a. [Conditional: TOE is a server] Modify at least one byte in the server’s nonce in the Server
- 1795 Hello handshake message, and verify that the server denies the client’s Finished
- 1796 handshake message.
  
- 1797 b. [Conditional: TOE is a client] Modify the server’s selected ciphersuite in the Server Hello
- 1798 handshake message to be a ciphersuite not presented in the Client Hello handshake
- 1799 message. The evaluator shall verify that the client rejects the connection after receiving
- 1800 the Server Hello.
  
- 1801 c. [Conditional: TOE is a client] If a DHE or ECDHE ciphersuite is supported, modify the
- 1802 signature block in the Server’s KeyExchange handshake message, and verify that the client
- 1803 rejects the connection after receiving the Server KeyExchange.
  
- 1804 d. [Conditional: TOE is a client] Modify a byte in the Server Finished handshake message,
- 1805 and verify that the client sends a fatal alert upon receipt and does not send any
- 1806 application data.

6.5 Class FDP: User Data Protection

**Application Note:**

The User Data Access Control SFP is composed of Table 20, Table 21, FDP\_ACC.1, FDP\_ACF.1, FMT\_MSA.1, and FMT\_MSA.3.

		"Create"	"Read"	"Modify"	"Delete"
Print (+PRT)	<b>Operation:</b>	<b>Submit a document to be printed</b>	<b>View image or Release printed output</b>	<b>Modify stored document</b>	<b>Delete stored document</b>
	<b>Job owner</b>	Allowed (note 1)	View: no function Release: allowed	No function	Allowed
	<b>U.ADMIN</b>	No function	View: no function Release: allowed	No function	Allowed
	<b>U.NORMAL</b>	Allowed	Denied	Denied	Denied
	<b>Unauthenticated</b>	(condition 1)	Denied	Denied	Denied
Scan (+SCN)	<b>Operation:</b>	<b>Submit a document for scanning</b>	<b>View scanned image</b>	<b>Modify stored image</b>	<b>Delete stored image</b>
	<b>Job owner</b>	Allowed (note 2)	No function	No function	Allowed
	<b>U.ADMIN</b>	No function	No function	No function	Allowed
	<b>U.NORMAL</b>	Allowed	Denied	Denied (No function)	Denied (No function)
	<b>Unauthenticated</b>	Denied	Denied	Denied (No function)	Denied (No function)

		"Create"	"Read"	"Modify"	"Delete"
<b>Copy (+CPY)</b>	<b>Operation:</b>	<b>Submit a document for copying</b>	<b>View scanned image or Release printed copy output</b>	<b>Modify stored image</b>	<b>Delete stored image</b>
	<b>Job owner</b>	Allowed (note 2)	View: no function Release: no function	No function	Allowed
	<b>U.ADMIN</b>	No function	View: no function Release: no function	No function	Allowed
	<b>U.NORMAL</b>	Allowed	Denied	Denied (No function)	Denied (No function)
	<b>Unauthenticated</b>	Denied	Denied	Denied (No function)	Denied (No function)
<b>Fax send (+FAXOUT)</b>	<b>Operation:</b>	<b>Submit a document to send as a fax</b>	<b>View scanned image</b>	<b>Modify stored image</b>	<b>Delete stored image</b>
	<b>Job owner</b>	Allowed (note 2)	No function	No function	Allowed
	<b>U.ADMIN</b>	No function	No function	No function	Allowed
	<b>U.NORMAL</b>	Allowed	Denied	Denied (No function)	Denied (No function)
	<b>Unauthenticated</b>	Denied	Denied	Denied (No function)	Denied (No function)
<b>Fax receive (+FAXIN)</b>	<b>Operation:</b>	<b>Receive a fax and store it</b>	<b>View fax image or Release printed fax output</b>	<b>Modify image of received fax</b>	<b>Delete image of received fax</b>
	<b>Fax owner</b>	Allowed (note 3)	View: allowed Release: allowed	No function	Allowed
	<b>U.ADMIN</b>	Allowed (note 4)	View: no function Release: no function	No function	No function
	<b>U.NORMAL</b>	Allowed (note 4)	Denied	Denied	Denied
	<b>Unauthenticated</b>	Allowed	Denied	Denied	Denied
<b>Storage / retrieval (+DSR)</b>	<b>Operation:</b>	<b>Store document</b>	<b>Retrieve stored document</b>	<b>Modify stored document</b>	<b>Delete stored document</b>
	<b>Job owner</b>	Allowed (note 1)	Allowed	Allowed	Allowed
	<b>U.ADMIN</b>	No function	Denied	Allowed	Allowed
	<b>U.NORMAL</b>	Allowed	Denied	Denied	Denied
	<b>Unauthenticated</b>	(condition 1)	Denied	Denied	Denied

1812 Table 20 D.USER.DOC Access Control SFP

1813

		"Create" *	"Read"	"Modify"	"Delete"
Print (+PRT)	<b>Operation:</b>	<b>Create print job</b>	<b>View print queue / log</b>	<b>Modify print job</b>	<b>Cancel print job</b>
	Job owner	(note 1)	Allowed	No function	Allowed
	U.ADMIN	No function	Allowed	No function	Allowed
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Allowed	Allowed	Denied	Denied
Scan (+SCN)	<b>Operation:</b>	<b>Create scan job</b>	<b>View scan status / log</b>	<b>Modify scan job</b>	<b>Cancel scan job</b>
	Job owner	(note 2)	Allowed	No function	Allowed
	U.ADMIN	No function	Allowed	No function	Allowed
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Copy (+CPY)	<b>Operation:</b>	<b>Create copy job</b>	<b>View copy status / log</b>	<b>Modify copy job</b>	<b>Cancel copy job</b>
	Job owner	(note 2)	Allowed	No function	Allowed
	U.ADMIN	No function	Allowed	No function	Allowed
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Fax send (+FAXOUT)	<b>Operation:</b>	<b>Create fax send job</b>	<b>View fax job queue / log</b>	<b>Modify fax send job</b>	<b>Cancel fax send job</b>
	Job owner	(note 2)	Allowed	Allowed	Allowed
	U.ADMIN	No function	Allowed	No function	Allowed
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	Denied	Denied	Denied	Denied
Fax receive (+FAXIN)	<b>Operation:</b>	<b>Create fax receive job</b>	<b>View fax receive status / log</b>	<b>Modify fax receive job</b>	<b>Cancel fax receive job</b>
	Fax owner	(note 3)	Allowed	No function	Allowed
	U.ADMIN	(note 4)	Allowed	No function	Allowed
	U.NORMAL	(note 4)	Allowed	Denied	Denied
	Unauthenticated	Allowed	Denied	Denied	Denied
Storage / retrieval (+DSR)	<b>Operation:</b>	<b>Create storage / retrieval job</b>	<b>View storage / retrieval log</b>	<b>Modify storage / retrieval job</b>	<b>Cancel storage / retrieval job</b>
	Job owner	(note 1)	Allowed	No function	No function
	U.ADMIN	No function	Allowed	No function	No function
	U.NORMAL	Allowed	Allowed	Denied	Denied
	Unauthenticated	(condition 1)	Denied	Denied	Denied

1814 Table 21 D.USER.JOB Access Control SFP

1815 **Application note:**

1816 *In general, the ST Author may modify this SFP provided that any changes are more restrictive. As*  
1817 *examples, the ST Author may: remove the rules related to Document Processing functions that are not*  
1818 *present in a TOE, add or modify rules to further deny access, or subdivide User Data to further restrict*  
1819 *access for some data (e.g., D.USER.JOB.PROT and D.USER.JOB.CONF). Empty cells in the table indicate that*  
1820 *the operation may be permitted, but it is not required to be permitted.*

1821 *In particular, referring to Table 20 and Table 21:*

1822 *A cell marked “Denied” indicates that the user (row) must not be permitted to perform the operation*  
1823 *(column). The ST Author cannot override this.*

1824 *A cell that is blank indicates that the user may be permitted to perform the operation. However, the ST*  
1825 *author may add conditions or restrictions, or deny permission entirely.*

1826 *A cell that is marked with a Condition means that the user can be permitted to perform the operation,*  
1827 *provided that it meets that Condition as specified below. As with blank cells, the ST author can make it*  
1828 *more restrictive.*

1829 **Condition 1:** *Jobs submitted by unauthenticated users must contain a credential that the TOE can use to*  
1830 *identify the Job Owner.*

1831 *See also the following Notes that are referenced in Table 20 and Table 21:*

1832 **Note 1:** *Job Owner is identified by a credential or assigned to an authorized User as part of the process of*  
1833 *submitting a print or storage Job.*

1834 **Note 2:** *Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax*  
1835 *send, or retrieval Job.*

1836 **Note 3:** *Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of*  
1837 *received faxes is assigned to a specific user or U.ADMIN role.*

1838 **Note 4:** *PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.*

### 1839 6.5.1 FDP\_ACC.1 Subset access control

1840 (for O.ACCESS\_CONTROL and O.USER\_AUTHORIZATION)

1841 Hierarchical to: No other components.

1842 Dependencies: FDP\_ACF.1 Security attribute based access control

1843 **FDP\_ACC.1.1 Refinement:** *The TSF shall enforce the User Data Access Control SFP on subjects, objects, and*  
1844 *operations among subjects and objects specified in Table 20 and Table 21.*

#### 1845 **Application note:**

1846 *Refer to the Application Note associated with Table 20 and Table 21.*

#### 1847 **Assurance Activity:**

1848 It is covered by assurance activities for FDP\_ACF.1.

1849 **6.5.2 FDP\_ACF.1 Security attribute based access control**

1850 (for O.ACCESS\_CONTROL and O.USER\_AUTHORIZATION)

1851 Hierarchical to: No other components.

1852 Dependencies: FDP\_ACC.1 Subset access control

1853 FMT\_MSA.3 Static attribute initialization

1854 **FDP\_ACF.1.1 Refinement:** The TSF shall enforce the **User Data Access Control SFP** to objects based on the  
1855 following: **subjects, objects, and attributes specified in Table 20 and Table 21.**

1856 **FDP\_ACF.1.2 Refinement:** The TSF shall enforce the following rules to determine if an operation among  
1857 controlled subjects and controlled objects is allowed: [**rules governing access among controlled subjects and**  
1858 **controlled objects using controlled operations on controlled objects specified in Table 20 and Table 21**].

1859 **FDP\_ACF.1.3 Refinement:** The TSF shall explicitly authorize access of subjects to objects based on the following  
1860 additional rules: [**no additional rules**].

1861 **FDP\_ACF.1.4 Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following  
1862 additional rules: [**all controlled operations on controlled objects specified in Table 20 and Table 21 are**  
1863 **explicitly denied to U.ADMIN.SUP**].

1864 **Assurance Activity:**

1865 TSS:

1866 The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 20  
1867 and Table 21 by providing specific details so that ST readers can understand without being  
1868 misunderstood.

1869 *Operational Guidance:*

1870 The evaluator shall check to ensure that the operational guidance contains a description of the operation  
1871 to realize the SFP defined in Table 20 and Table 21, which is consistent with the description in the TSS.

1872 *Test:*

1873 The evaluator shall perform tests to confirm the functions to realize the SFP defined in Table 20 and Table  
1874 21 with each type of interface (e.g., operation panel, Web interfaces) to the TOE.

1875 The evaluator testing should include the following viewpoints:

- 1876
- representative sets of the operations against all the object types defined in Table 20 and Table 21  
1877 (including some cases where operations are either permitted or denied)
  - representative sets for the combinations of the setting for security attributes that are used in  
1878 access control  
1879

1880 **6.5.3 FDP\_DSK\_EXT.1 Extended: Protection of Data on Disk**

1881 (for O.STORAGE\_ENCRYPTION)

1882 Hierarchical to: No other components.

1883 Dependencies: FCS\_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).

1884 **FDP\_DSK\_EXT.1.1** The TSF shall [*perform encryption in accordance with FCS\_COP.1(d)*], such that any Field-  
1885 Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext  
1886 Confidential TSF Data.

1887 **Application Note:**

1888 *If the self-encrypting device option is selected, the device must be certified in conformance to the current*  
1889 *Full Disk Encryption Protection Profile. The ST Author should consult with a CC Scheme for advice on*  
1890 *approved Protection Profiles.*

1891 **FDP\_DSK\_EXT.1.2** The TSF shall encrypt all protected data without user intervention.

1892 **Application Note:**

1893 *The intent of this requirement is to specify that encryption of any confidential data will not depend on a*  
1894 *user electing to protect that data. The encryption specified in FDP\_DSK\_EXT.1 occurs transparently to the*  
1895 *user and the decision to protect the data is outside the discretion of the user.*

1896 **Assurance activity:**

1897 In the assurance activities, below, “Device” refers to the Field-Replaceable Nonvolatile Storage Device  
1898 from FDP\_DSK\_EXT.1. If the TOE contains more than one applicable Device, then the assurance activities  
1899 are performed as necessary on each such Device.

1900 **TSS:**

1901 The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is  
1902 written to the Device and the point at which the encryption function is applied.

1903 For the cryptographic functions that are provided by the Operational Environment, the evaluator shall  
1904 check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality.

1905 The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or  
1906 by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user  
1907 or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the  
1908 Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition  
1909 tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the  
1910 administration guidance to ensure the initialization procedure encrypts all Devices.

1911 **Operational Guidance:**

1912 The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to  
1913 enable the Device encryption function, including any necessary preparatory steps. The guidance shall  
1914 provide instructions that are sufficient to ensure that all Devices will be encrypted when encryption is  
1915 enabled or at shipment of the TOE.

1916 **KMD:**

1917 The evaluator shall verify the KMD includes a description of the data encryption engine, its components,  
1918 and details about its implementation (e.g. for hardware: integrated within the device’s main SOC or  
1919 separate co-processor, for software: initialization of the Device, drivers, libraries (if applicable), logical



1920 interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions that  
1921 do not contain confidential data, partition tables, etc.)). The evaluator shall verify the KMD provides a  
1922 functional (block) diagram showing the main components (such as memories and processors) and the  
1923 data path between, for hardware, the Device's interface and the Device's persistent media storing the  
1924 data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the  
1925 storage device entirely when a user or administrator first provisions the product. The hardware  
1926 encryption diagram shall show the location of the data encryption engine within the data path. The  
1927 evaluator shall validate that the hardware encryption diagram contains enough detail showing the main  
1928 components within the data path and that it clearly identifies the data encryption engine.

1929 The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is  
1930 enabled, the TOE encrypts all applicable Devices. The evaluator shall verify that the KMD describes the  
1931 data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify  
1932 that the KMD provides information on those conditions in which the data bypasses the data encryption  
1933 engine (e.g. read-write operations to an unencrypted area).

1934 The evaluator shall verify that the KMD provides a description of the boot initialization, the encryption  
1935 initialization process, and at what moment the product enables the encryption. If encryption can be  
1936 enabled and disabled, the evaluator shall validate that the product does not allow for the transfer of  
1937 confidential data before it fully initializes the encryption. The evaluator shall ensure the software  
1938 developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-  
1939 band, and may allow provisioning with a known key.

1940 *Test:*

1941 The evaluator shall perform the following tests:

1942 **Test 1.** Write data to Storage device: Perform writing to the storage device with operating TSFI which  
1943 enforce write process of User documents and Confidential TSF data.

1944 **Test 2.** Confirm that written data are encrypted: Verify there are no plaintext data present in the  
1945 encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key  
1946 material.

1947 All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and  
1948 Test 2.

#### 1949 **6.5.4 FDP\_FXS\_EXT.1 Extended: Fax separation**

1950 (for O.FAX\_NET\_SEPARATION)

1951 Hierarchical to: No other components.

1952 Dependencies: No dependencies.

1953 **FDP\_FXS\_EXT.1.1** The TSF shall prohibit communication via the fax interface, except transmitting or receiving  
1954 User Data using fax protocols.

1955 **Application note:**

1956 *FDP\_FXS\_EXT.1 is required if fax-net separation is performed by the TSF.*



1957

**Assurance Activity:**

1958

The following assurance activities are required when the TOE has a fax communication function to transmit and receive via PSTN.

1959

1960

*TSS:*

1961

The evaluator shall check the TSS to ensure that it describes:

1962

1. The fax interface use cases

1963

2. The capabilities of the fax modem and the supported fax protocols

1964

3. The data that is allowed to be sent or received via the fax interface

1965

4. How the TOE can only be used transmitting or receiving User Data using fax protocols

1966

*Operational Guidance:*

1967

The evaluator shall check to ensure that the operational guidance contains a description of the fax interface in terms of usage and available features.

1968

1969

*Test:*

1970

The evaluator shall test to ensure that the fax interface can only be used transmitting or receiving User Data using fax protocols. Testing will be dependent upon how the TOE enforces this requirement. The following tests shall be used and supplemented with additional testing or a rationale as to why the following tests are sufficient:

1971

1972

1973

1974

1. Verify that the TOE accepts incoming calls using fax carrier protocols and rejects calls that use data carriers. For example, this may be achieved using a terminal application to issue modem commands directly to the TOE from a PC modem (issue terminal command: 'ATDT <TOE Fax Number>') – the TOE should answer the call and disconnect.

1975

1976

1977

1978

2. Verify TOE negotiates outgoing calls using fax carrier protocols and rejects negotiation of data carriers. For example, this may be achieved by using a PC modem to attempt to receive a call from the TOE (submit a fax job from the TOE to <PC modem number>, at PC issue terminal command: 'ATA') – the TOE should disconnect without negotiating a carrier.

1979

1980

1981

1982

### 6.5.5 FDP\_RIP.1(a) Subset residual information protection

1983

(for O.IMAGE\_OVERWRITE)

1984

Hierarchical to: No other components.

1985

Dependencies: No dependencies.

1986

**FDP\_RIP.1.1(a) Refinement:** The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting data** upon the **deallocation of the resource from** the following objects:

1987

1988

**D.USER.DOC.**

1989

**Assurance activity:**

1990

*TSS:*

---

1991 The evaluator shall examine the TSS to ensure that the description is comprehensive in describing where  
 1992 image data is stored and how and when it is overwritten.

1993 *Operational Guidance:*

1994 The evaluator shall check to ensure that the operational guidance contains instructions for enabling the  
 1995 Image Overwrite function.

1996 *Test:*

1997 The evaluator shall include tests related to this function in the set of tests performed in FMT\_SMF.1.

1998 **6.6 Class FIA: Identification and Authentication**

1999 **6.6.1 FIA\_AFL.1 Authentication failure handling**

2000 (for O.USER\_I&A)

2001 Hierarchical to: No other components.

2002 Dependencies: FIA\_UAU.1 Timing of authentication

2003 **FIA\_AFL.1.1** The TSF shall detect when [*an administrator configurable positive integer within [1 to 5]*]  
 2004 unsuccessful authentication attempts occur related to [*list of authentication events shown in Table 22*].

Authentication Events
User authentication using the Operation Panel
User authentication using WIM from the client computer
User authentication when printing from the client computer
User authentication when using LAN Fax from the client computer

2005 *Table 22 Authentication Events*

2006 **FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall  
 2007 [*perform actions shown in Table 23*].

Unsuccessfully Authenticated Users	Actions for Authentication Failure
Normal user	The lockout for the Normal User is released by the lockout time set by the MFP Administrator, or release operation by the MFP Administrator.
MFP Supervisor	The lockout for a MFP Supervisor is released by the lockout time set by the MFP Administrator, release operation by the MFP Administrator, or elapse of a given time after the TOE's restart.
MFP Administrator	The lockout for the MFP Administrator is released by the lockout time set by the MFP Administrator, release operation by a MFP Supervisor, or elapse of a given time after the TOE's restart.

2008 *Table 23 List of Actions for Authentication Failure*

2009 **Application note:**

2010 *This SFR applies only to internal identification and authentication.*

2011 **Assurance Activity:**

2012 *TSS:*

2013 The evaluator shall check to ensure that the TSS contains a description of the actions in the case of  
2014 authentication failure (types of authentication events, the number of unsuccessful authentication  
2015 attempts, actions to be conducted), which is consistent with the definition of the SFR.

2016 *Operational Guidance:*

2017 The evaluator shall check to ensure that the administrator guidance describes the setting for actions to be  
2018 taken in the case of authentication failure, if any are defined in the SFR.

2019 *Test:*

2020 The evaluator shall also perform the following tests:

- 2021 1. The evaluator shall check to ensure that the subsequent authentication attempts do not succeed  
2022 by the behavior according to the actions defined in the SFR when unsuccessful authentication  
2023 attempts reach the status defined in the SFR.
- 2024 2. The evaluator shall check to ensure that authentication attempts succeed when conditions to re-  
2025 enable authentication attempts are defined in the SFR and when the conditions are fulfilled.
- 2026 3. The evaluator shall perform the tests 1 and 2 described above for all the targeted authentication  
2027 methods when there are multiple Internal Authentication methods (e.g., password  
2028 authentication, biometric authentication).
- 2029 4. The evaluator shall perform the tests 1 and 2 described above for all interfaces when there are  
2030 multiple interfaces (e.g., operation panel, Web interfaces) that implement authentication  
2031 attempts.

## 2032 6.6.2 FIA\_ATD.1 User attribute definition

2033 (for O.USER\_AUTHORIZATION)

2034 Hierarchical to: No other components.

2035 Dependencies: No dependencies.

2036 **FIA\_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [**Login**  
2037 **User Name, User Role, Available Functions List**].

2038 **Application note:**

2039 *The list of security attributes should be the union of all attributes for each of the supported authentication*  
2040 *methods.*

2041 **Assurance Activity:**

2042 *TSS:*

2043 The evaluator shall check to ensure that the TSS contains a description of the user security attributes that  
2044 the TOE uses to implement the SFR, which is consistent with the definition of the SFR.

## 2045 6.6.3 FIA\_PMG\_EXT.1 Extended: Password Management

2046 (for O.USER\_I&A)

2047 Hierarchical to: No other components.

2048 Dependencies: No dependencies.

2049 **FIA\_PMG\_EXT.1.1** The TSF shall provide the following password management capabilities for User passwords:

- 2050 ▪ Passwords shall be able to be composed of any combination of upper and lower case letters, numbers,  
2051 and the following special characters: ["!", "@", "#", "\$", "%", "^", "&", "\*", "(", ")", ["'", "'"], ["'", "'"], "+", ";", "-",  
2052 ":", "/", ":", ";", "<", "=", ">", "?", "[", "\\", "]", "\_", "~", "{", "|", "}", "~"];
- 2053 ▪ Minimum password length shall be settable by an Administrator, and have the capability to require  
2054 passwords of 15 characters or greater;

2055 **Application Note:**

2056 *This SFR applies only to password-based single-factor Internal Authentication.*

2057 **Assurance Activity:**

2058 *Operational Guidance:*

2059 The evaluator shall examine the operational guidance to determine that it provides guidance to security  
2060 administrators on the composition of passwords, and that it provides instructions on setting the minimum  
2061 password length.

2062 *Test:*

2063 The evaluator shall also perform the following test:

2064 The evaluator shall compose passwords that either meet the requirements, or fail to meet the  
2065 requirements, in some way. For each password, the evaluator shall verify that the TOE supports the  
2066 password. While the evaluator is not required (nor is it feasible) to test all possible compositions of  
2067 passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed  
2068 in the requirement are supported, and justify the subset of those characters chosen for testing.

2069 **6.6.4 FIA\_PSK\_EXT.1 Extended: Pre-Shared Key Composition**

2070 (selected with FCS\_IPSEC\_EXT.1.4)

2071 Hierarchical to: No other components.

2072 Dependencies: FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

2073 **Application Note:**

2074 *The TOE must support pre-shared keys for use in the IPsec protocol. There are two types of pre-shared*  
2075 *keys--text-based (which are required) and bit-based (which are optional)--supported by the TOE, as*  
2076 *specified in the requirements below. The first type is referred to as "text-based pre-shared keys", which*  
2077 *refer to pre-shared keys that are entered by users as a string of characters from a standard character set,*  
2078 *similar to a password. Such pre-shared keys must be conditioned so that the string of characters is*  
2079 *transformed into a string of bits, which is then used as the key.*

2080 *The second type is referred to as "bit-based pre-shared keys" (for lack of a standard term); this refers to*  
2081 *keys that are either generated by the TSF on a command from the administrator, or input in "direct form"*  
2082 *by an administrator. "Direct form" means that the input is used directly as the key, with no "conditioning"*  
2083 *as was the case for text-based pre-shared keys. An example would be a string of hex digits that represent*  
2084 *the bits that comprise the key.*

2085            *The requirements below mandate that the TOE must support text-based pre-shared keys and optionally*  
2086            *support bit-based pre-shared keys, although generation of the bit-based pre-shared keys may be done*  
2087            *either by the TOE or in the Operational Environment.*

2088    **FIA\_PSK\_EXT.1.1** The TSF shall be able to use pre-shared keys for IPsec.

2089    **FIA\_PSK\_EXT.1.2** The TSF shall be able to accept text-based pre-shared keys that are:

- 2090    • 22 characters in length and **[[1-32 characters]]**;
- 2091    • composed of any combination of upper and lower case letters, numbers, and special characters (that  
2092    include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, and “”).

2093    **FIA\_PSK\_EXT.1.3** The TSF shall condition the text-based pre-shared keys by using **[SHA-256]** and be able to **[use**  
2094    **no other pre-shared keys]**.

2095    **Application Note:**

2096            *For the length of the text-based pre-shared keys, a common length (22 characters) is required to help*  
2097            *promote interoperability. If other lengths are supported they should be listed in the assignment; this*  
2098            *assignment can also specify a range of values (e.g., “lengths from 5 to 55 characters”) as well.*

2099            *In the second selection for FIA\_PSK\_EXT.1.3, the ST author fills in the method by which the text string*  
2100            *entered by the administrator is “conditioned” into the bit string used as the key. This can be done by using*  
2101            *one of the specified hash functions, or some other method through the assignment statement. If “bit-*  
2102            *based pre-shared keys” is selected, the ST author specifies whether the TSF merely accepts bit-based pre-*  
2103            *shared keys, or is capable of generating them. If it generates them, the requirement specified that they*  
2104            *must be generated using the RBG specified by the requirements. If the use of bit-based pre-shared keys is*  
2105            *not supported, the ST author chooses “use no other pre-shared keys”.*

2106    **Assurance Activity:**

2107            *Operational Guidance:*

2108            The evaluator shall examine the operational guidance to determine that it provides guidance on the  
2109            composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths  
2110            can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The  
2111            guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of  
2112            the list contained in FIA\_PSK\_EXT.1.2.

2113            *TSS:*

2114            The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22  
2115            characters are supported, and that the TSS states the conditioning that takes place to transform the text-  
2116            based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit  
2117            string used by IPsec, and that this conditioning is consistent with the first selection in the FIA\_PSK\_EXT.1.3  
2118            requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS  
2119            describes this conditioning.

2120            If “bit-based pre-shared keys” is selected, the evaluator shall confirm the operational guidance contains  
2121            instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement,

2122 or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it  
2123 describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this  
2124 functionality), and confirm that this process uses the RBG specified in FCS\_RBG\_EXT.1.

2125 *Test:*

2126 The evaluator shall also perform the following tests:

2127 1. The evaluator shall compose at least 15 pre-shared keys of 22 characters that cover all allowed  
2128 characters in various combinations that conform to the operational guidance, and demonstrates that a  
2129 successful protocol negotiation can be performed with each key.

2130 2. [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1  
2131 using the minimum length; the maximum length; and an invalid length. The minimum and maximum  
2132 length tests should be successful, and the invalid length must be rejected by the TOE.

2133 3. [conditional]: If the TOE supports bit-based pre-shared keys but does not generate such keys, the  
2134 evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the  
2135 instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol  
2136 negotiation can be performed with the key.

2137 4. [conditional]: If the TOE supports bit-based pre-shared keys and does generate such keys, the evaluator  
2138 shall generate a bit-based pre-shared key of the appropriate length and use it according to the  
2139 instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol  
2140 negotiation can be performed with the key.

#### 2141 6.6.5 FIA\_UAU.1 Timing of authentication

2142 (for O.USER\_I&A)

2143 Hierarchical to: No other components.

2144 Dependencies: FIA\_UID.1 Timing of identification

2145 **FIA\_UAU.1.1 Refinement:** The TSF shall allow [*the viewing of the list of user jobs, WIM Help, system status,*  
2146 *counter and information of inquiries, and creation of fax reception and print jobs*] on behalf of the user to  
2147 be performed before the user is authenticated.

2148 **FIA\_UAU.1.2** The TSF shall require each user to be successfully authenticated before allowing any other TSF-  
2149 mediated actions on behalf of that user.

#### 2150 **Application note:**

2151 *User authentication may be performed internally by the TOE or externally by an External IT Entity.*

#### 2152 **Assurance Activity:**

2153 *TSS:*

2154 The evaluator shall check to ensure that the TSS describes all the identification and authentication  
2155 mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers).

2156 The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and  
2157 authentication (e.g., identification and authentication from operation panel or via Web interfaces).

2158 The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used  
2159 in performing identification and authentication when the TOE exchanges identification and authentication  
2160 with External Authentication servers.

2161 The evaluator shall check to ensure that the TSS contains a description of the permitted actions before  
2162 performing identification and authentication, which is consistent with the definition of the SFR.

2163 *Operational Guidance:*

2164 The evaluator shall check to ensure that the administrator guidance contains descriptions of identification  
2165 and authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication)  
2166 as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces),  
2167 which are consistent with the ST (TSS).

2168 *Test:*

2169 The evaluator shall also perform the following tests:

- 2170 1. The evaluator shall check to ensure that identification and authentication succeeds, enabling the  
2171 access to the TOE when using authorized data.
- 2172 2. The evaluator shall check to ensure that identification and authentication fails, disabling the  
2173 access to the TOE afterwards when using unauthorized data.

2174 The evaluator shall perform the tests described above for each of the authentication methods that the  
2175 TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g.,  
2176 identification and authentication from operation panel or via Web interfaces).

#### 2177 6.6.6 FIA\_UAU.7 Protected authentication feedback

2178 (for O.USER\_I&A)

2179 Hierarchical to: No other components.

2180 Dependencies: FIA\_UAU.1 Timing of authentication

2181 **FIA\_UAU.7.1** The TSF shall provide only [*displaying dummy characters as authentication feedback on the*  
2182 *Operation Panel and through WIM*] to the user while the authentication is in progress.

2183 ***Application note:***

2184 *FIA\_UAU.7 applies only to authentication processes in which the User interacts with the TOE.*

2185 **Assurance Activity:**

2186 *TSS:*

2187 The evaluator shall check to ensure that the TSS contains a description of the authentication information  
2188 feedback provided to users while the authentication is in progress, which is consistent with the definition  
2189 of the SFR.

2190 *Test:*

2191 The evaluator shall also perform the following tests:



- 2192 1. The evaluator shall check to ensure that only the information defined in the SFR is provided for  
 2193 feedback by attempting identification and authentication.
- 2194 2. The evaluator shall perform the test 1 described above for all the interfaces that the TOE provides  
 2195 (e.g., operation panel, identification and authentication via Web interface).

2196 **6.6.7 FIA\_UID.1 Timing of identification**

2197 (for O.USER\_I&A and O.ADMIN\_ROLES)

2198 Hierarchical to: No other components.

2199 Dependencies: No dependencies.

2200 **FIA\_UID.1.1 Refinement:** The TSF shall allow [*the viewing of the list of user jobs, WIM Help, system status,*  
 2201 *counter and information of inquiries, creation of fax reception jobs, and creation of print jobs*] on behalf of  
 2202 the user to be performed before the user is identified.

2203 **FIA\_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated  
 2204 actions on behalf of that user.

2205 **Application note:**

2206 *User identification may be performed internally by the TOE or externally by an External IT Entity.*

2207 **Assurance Activity:**

2208 It is covered by assurance activities for FIA\_UAU.1.

2209 **6.6.8 FIA\_USB.1 User-subject binding**

2210 (for O.USER\_I&A)

2211 Hierarchical to: No other components.

2212 Dependencies: FIA\_ATD.1 User attribute definition

2213 **FIA\_USB.1.1** The TSF shall associate the following user security attributes with subjects acting on the behalf of  
 2214 that user: [*login user name of Normal User, login user name of MFP Administrator, login user name of MFP*  
 2215 *Supervisor, available function list, and user role*].

2216 **FIA\_USB.1.2** The TSF shall enforce the following rules on the initial association of user security attributes with  
 2217 subjects acting on the behalf of users: [*rules for the initial association of attributes listed in Table 24*].

Users	Subjects	User Security Attributes
Normal user	Normal user process	Login user name of Normal User User role Available functions list
MFP Administrator	MFP Administrator process	Login user name of MFP Administrator User role Available functions list (none for Administrators)
MFP Supervisor	MFP Supervisor process	Login user name of MFP Supervisor User role Available functions list (none for Administrators)

2218 *Table 24 Rules for Initial Association of Attributes*



2219 **FIA\_USB.1.3** The TSF shall enforce the following rules governing changes to the user security attributes  
2220 associated with subjects acting on the behalf of users: [*none*].

2221 **Assurance Activity:**

2222 *TSS:*

2223 The evaluator shall check to ensure that the TSS contains a description of rules for associating security  
2224 attributes with the users who succeed identification and authentication, which is consistent with the  
2225 definition of the SFR.

2226 *Test:*

2227 The evaluator shall also perform the following test:

2228 The evaluator shall check to ensure that security attributes defined in the SFR are associated with the  
2229 users who succeed identification and authentication (it is ensured in the tests of FDP\_ACF) for each role  
2230 that the TOE supports (e.g., User and Administrator).

## 2231 6.7 Class FMT: Security Management

### 2232 6.7.1 FMT\_MOF.1 Management of security functions behavior

2233 (for O.ADMIN\_ROLES)

2234 Hierarchical to: No other components.

2235 Dependencies: FMT\_SMR.1 Security roles

2236 FMT\_SMF.1 Specification of Management Functions

2237 **FMT\_MOF.1.1 Refinement:** The TSF shall restrict the ability to [*determine the behavior of, enable, disable,*  
2238 *modify the behavior of*] the functions [*listed in Table 26*] to U.ADMIN.

2239 **Assurance Activity:**

2240 *TSS:*

2241 The evaluator shall check to ensure that the TSS contains a description of the management functions that  
2242 the TOE provides as well as user roles that are permitted to manage the functions, which is consistent  
2243 with the definition of the SFR.

2244 The evaluator shall check to ensure that the TSS identifies interfaces to operate the management  
2245 functions.

2246 *Operational Guidance:*

2247 The evaluator shall check to ensure that the administrator guidance describes the operation methods for  
2248 users of the given roles defined in the SFR to operate the management functions.

2249 *Test:*

2250 The evaluator shall also perform the following tests:

- 2251 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can operate  
 2252 the management functions in accordance with the operation methods specified in the  
 2253 administrator guidance.
- 2254 2. The evaluator shall check to ensure that the operation results are appropriately reflected.
- 2255 3. The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management  
 2256 functions.

2257 **6.7.2 FMT\_MSA.1 Management of security attributes**

2258 (for O.ACCESS\_CONTROL and O.USER\_AUTHORIZATION)

2259 Hierarchical to: No other components.

2260 Dependencies: [FDP\_ACC.1 Subset access control]

2261 FMT\_SMR.1 Security roles

2262 FMT\_SMF.1 Specification of Management Functions

2263 **FMT\_MSA.1.1 Refinement:** The TSF shall enforce the User Data Access Control SFP to restrict the ability to  
 2264 [[*perform operations specified in Table 25*]] the security attributes [*listed in Table 25*] to [*the roles identified*  
 2265 *in Table 25*].

Security Attribute(s)	Operation(s)	User Role
Document data attribute	No operation permitted	None
Document user list [when document data attributes are (+PRT), (+SCN), (+CPY), and (+FAXOUT)]	No operation permitted	None
Document user list [when document data attribute is (+DSR)]	Query, modify	MFP Administrator, applicable Normal User who created the document data
Document user list [when document data attribute is (+FAXIN)]	Query, modify	MFP Administrator

2266 *Table 25 User Roles for Security Attributes*

2267 **Assurance Activity:**

2268 TSS:

2269 The evaluator shall check to ensure that the TSS contains a description of possible operations for security  
 2270 attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

2271 *Operational Guidance:*

2272 The evaluator shall check to ensure that the administrator guidance contains a description of possible  
 2273 operations for security attributes and given roles to those security attributes, which is consistent with the  
 2274 definition of the SFR.

2275 The evaluator shall check to ensure that the administrator guidance describes the timing of modified  
 2276 security attributes.

2277 *Test:*

2278 The evaluator shall also perform the following tests:

- 2279 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform  
2280 operations to the security attributes in accordance with the operation methods specified in the  
2281 administrator guidance.
- 2282 2. The evaluator shall check to ensure that the operation results are appropriately reflected as  
2283 specified in the administrator guidance.
- 2284 3. The evaluator shall check to ensure that a user that is not part of an authorized role defined in the  
2285 SFR is not permitted to perform operations on the security attributes.

### 2286 6.7.3 FMT\_MSA.3 Static attribute initialization

2287 (for O.ACCESS\_CONTROL and O.USER\_AUTHORIZATION)

2288 Hierarchical to: No other components.

2289 Dependencies: FMT\_MSA.1 Management of security attributes

2290 FMT\_SMR.1 Security roles

2291 **FMT\_MSA.3.1 Refinement:** The TSF shall enforce the User Data Access Control SFP to provide [*restrictive*]  
2292 default values for security attributes that are used to enforce the SFP.

2293 **FMT\_MSA.3.2 Refinement:** The TSF shall allow the [*U.ADMIN*] to specify alternative initial values to override the  
2294 default values when an object or information is created.

#### 2295 **Application note:**

2296 *FMT\_MSA.3.2 applies only to security attributes whose default values can be overridden.*

#### 2297 **Assurance Activity:**

2298 *TSS:*

2299 The evaluator shall check to ensure that the TSS describes mechanisms to generate security attributes  
2300 which have properties of default values, which are defined in the SFR.

2301 *Test:*

2302 If U.ADMIN is selected, then testing of this SFR is performed in the tests of FDP\_ACF.1.

### 2303 6.7.4 FMT\_MTD.1 Management of TSF data

2304 (for O.ACCESS CONTROL)

2305 Hierarchical to: No other components.

2306 Dependencies: FMT\_SMR.1 Security roles

2307 FMT\_SMF.1 Specification of Management Functions

2308 **FMT\_MTD.1.1 Refinement:** The TSF shall restrict the ability to **perform the specified operations on the**  
2309 **specified TSF Data to the roles specified in Table 26 and Table 27.**

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
Access control	Document user list for stored document types +DSR and +FAXIN	D . T S F . P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Default values of the document user list	D . T S F . P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Available function list	D · T S F · P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator
<b>Audit function</b>	Audit log	D · T S F · C O N F	W e b b r o w s e r	Query, delete, export	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Audit transfer settings	D · T S F · P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Date settings (year/month/day), Time	D . T S F . P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator
<b>Identification and Authentication</b>	Minimum character number of password	D . T S F . P R O T	O p e r a t i o n P a n e l	Modify	MFP Administrator



Area	TSF Data	T I n t e r f a c e ( s )	Operation	Authorized role(s)
	Password complexity setting	D · T S F · P R O n P a n e l	O p e r a t i o n M o d i f y	MFP Administrator
	Operation Panel auto logout time	D · T S F · P R O n P a n e l	O p e r a t i o n M o d i f y	MFP Administrator
	WIM auto logout time	D · T S F · P R O n P a n e l	W e b b r o w s e r	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login user names of Normal Users	D . T S F . P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Create, modify, delete	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login user name of MFP Supervisor	D . T S F . P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Supervisor

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login user name of MFP Administrator	D . T S F . P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator (Owner)

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login passwords of Normal Users	D · T S F · C O N F	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login password of MFP Supervisor	D · T S F · C O N F	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Supervisor

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login password of MFP Administrator	D · T S F · C O N F	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Supervisor

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login password of MFP Administrator	D · T S F · C O N F	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator (Owner)



Area	TSF Data	T I n t e r f a c e ( s )	Operation	Authorized role(s)
	Login password of MFP Administrator	D O T S F C O N F P a n e l , W e b b r o w s e r	Modify	MFP Administrator
	Number of Attempts before Lockout	D W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Settings for Lockout Release Timer	D T S F P R O T	W e b b r o w s e r	Modify	MFP Administrator
	Lockout time	D T S F P R O T	W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T I n t e r f a c e ( s )	Operation	Authorized role(s)
<b>PSTN Fax-Line Separation</b>	Stored Reception File User	D O P T S R F P R O N P a n e l , W e b b r o w s e r	Modify	MFP Administrator
<b>Stored Data Encryption</b>	HDD cryptographic key	D O P T S R F C O N F P a n e l	Create, delete	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
Trusted communications	Network Settings	D O T S F P R O T	O p e r a t i o n P a n e l , W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	T y p e	I n t e r f a c e ( s )	Operation	Authorized role(s)
	Device Certificate	D · T S F · C O N F	O p e r a t i o n P a n e l , W e b b r o w s e r	Create, query, modify, delete	MFP Administrator
Trusted operations	TOE Software	D · T S F · P R O T	W e b b r o w s e r	Modify	MFP Administrator

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Multiple areas	TOE configuration data	DTSPROT	Web browser	Export, import	MFP Administrator

2310 Table 26 List of Administrator-only TSF Data, Operations, and Roles

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Access control	Document user list for stored document type +DSR	DTSPROT	Operation Panel, Web browser	Modify	MFP Administrator, Normal User (Owner) who stored the document
	Available function list	DTSPROT	Web browser	Query	Normal User (Owner)

Area	TSF Data	Type	Interface(s)	Operation	Authorized role(s)
Identification and Authentication	Login passwords of Normal Users	DISCONF	Operation Panel, Web browser	Modify	Normal User (Owner)

2311 Table 27 List of Additional TSF Data, Operations, and Roles

2312 **Note for Evaluators:** If a +PRT or +SCN document is stored in the document server, the act of storing is a +DSR  
 2313 job and the attribute of the stored document becomes +DSR.

2314 **Assurance Activity:**

2315 *Operational Guidance:*

2316 The evaluator shall check to ensure that the administrator guidance identifies the management  
 2317 operations and authorized roles consistent with the SFR.

2318 The evaluator shall check to ensure that the administrator guidance describes how the assignment of  
 2319 roles is managed.

2320 The evaluator shall check to ensure that the administrator guidance describes how security attributes are  
 2321 assigned and managed.

2322 The evaluator shall check to ensure that the administrator guidance describes how the security-related  
 2323 rules (e.g., access control rules, timeout, number of consecutive logon failures,) are configured.

2324 *Test:*

2325 The evaluator shall perform the following tests:

- 2326 • The evaluator shall check to ensure that users of the given roles defined in the SFR can perform  
 2327 operations to TSF data in accordance with the operation methods specified in the administrator  
 2328 guidance.
- 2329 • The evaluator shall check to ensure that the operation results are appropriately reflected as  
 2330 specified in the administrator guidance.
- 2331 • The evaluator shall check to ensure that no users other than users of the given roles defined in  
 2332 the SFR can perform operations to TSF data.

2333 **6.7.5 FMT\_SMF.1 Specification of Management Functions**

2334 (for O.USER\_AUTHORIZATION, O.ACCESS\_CONTROL, and O.ADMIN\_ROLES)

2335 Hierarchical to: No other components.

2336 Dependencies: No dependencies.

2337 **FMT\_SMF.1.1:** The TSF shall be capable of performing the following management functions: [*management*  
2338 *functions listed in Table 26*].

2339 **Application note:**

2340 *Regarding “management functions provided by the TSF”, the ST Author should consider management*  
2341 *functions that support the security objectives of this protection profile.*

2342 *The management functions should be restricted to the authorized identified role in FMT\_MOF.1,*  
2343 *FMT\_MTD.1, FMT\_MSA.1.*

2344 *The ST Author may identify cases where a security objective is fulfilled without explicit manageability.*

2345 *For example, the following management functions are categorized by security objectives:*

2346 *For O.USER\_AUTHORIZATION, O.USER\_I&A, O.ADMIN\_ROLES, O.ACCESS\_CONTROL:*

- 2347 • *User management (e.g., add/change/remove local user)*
- 2348 • *Role management (e.g., assign/deassign role relationship with user)*
- 2349 • *Configuring identification and authentication (e.g., selecting between local and external I&A)*
- 2350 • *Configuring authorization and access controls (e.g., access control lists for TOE resources)*

2351 *Configuring communication with External IT Entities*

2352 *For O.UPDATE\_VERIFICATION:*

- 2353 • *Configuring software updates*

2354 *For O.COMMS\_PROTECTION:*

- 2355 • *Configuring network communications*
- 2356 • *Configuring the system or network time source*

2357 *For O.AUDIT:*

- 2358 • *Configuring data transmission to audit server*
- 2359 • *Configuring the system or network time source*
- 2360 • *Configuring internal audit log storage*

2361 *For O.STORAGE\_ENCRYPTION, O.KEY\_MATERIAL:*

- 2362 • *Configuring and invoking encryption of Field-Replaceable Nonvolatile Storage Devices*

2363 *(Optional) For O.IMAGE\_OVERWRITE, O.PURGE DATA:*

- 2364 • *Configuring and/or invoking image overwrite functions*
- 2365 • *Configuring and/or invoking data purging functions*



2366

**Assurance Activity:**

2367

*TSS:*

2368

The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.

2369

2370

*Operational Guidance:*

2371

The evaluator shall check the guidance documents to ensure that management functions are consistent with the assignment in the SFR, and that their operation is described.

2372

2373

**6.7.6 FMT\_SMR.1 Security roles**

2374

(for O.ACCESS\_CONTROL, O.USER\_AUTHORIZATION, and O.ADMIN\_ROLES)

2375

Hierarchical to: No other components.

2376

Dependencies: FIA\_UID.1 Timing of identification

2377

**FMT\_SMR.1.1 Refinement:** The TSF shall maintain the roles U.ADMIN, U.NORMAL.

2378

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

2379

**Assurance Activity:**

2380

*TSS:*

2381

The evaluator shall check to ensure that the TSS contains a description of security related roles that the TOE maintains, which is consistent with the definition of the SFR.

2382

2383

*Test:*

2384

As for tests of this SFR, it is performed in the tests of FMT\_MOF.1, FMT\_MSA.1, and FMT\_MTD.1.

2385

**6.8 Class FPR: Privacy**

2386

There are no class FPR requirements.

2387

**6.9 Class FPT: Protection of the TSF**

2388

**6.9.1 FPT\_KYP\_EXT.1 Extended: Protection of Key and Key Material**

2389

(for O.KEY\_MATERIAL)

2390

Hierarchical to: No other components.

2391

Dependencies: No dependencies.

2392

**FPT\_KYP\_EXT.1.1 Refinement:** The TSF shall not store plaintext keys that are part of the keychain specified by FCS\_KYC\_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

2393

2394

**Assurance Activity:**

2395

*KMD:*

2396

The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory.

2397

2398 The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the  
2399 protection of all keys stored in nonvolatile memory.

## 2400 6.9.2 FPT\_SKP\_EXT.1 Extended: Protection of TSF Data

2401 (for O.COMMS\_PROTECTION)

2402 Hierarchical to: No other components.

2403 Dependencies: No dependencies.

2404 **FPT\_SKP\_EXT.1.1** The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

### 2405 **Application Note:**

2406 *The intent of the requirement is that an administrator is unable to read or view the identified keys (stored*  
2407 *or ephemeral) through “normal” interfaces. While it is understood that the administrator could directly*  
2408 *read memory to view these keys, doing so is not a trivial task and may require substantial work on the part*  
2409 *of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not*  
2410 *engage in such an activity.*

### 2411 **Assurance Activity:**

2412 TSS:

2413 The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys,  
2414 and private keys are stored and that they are unable to be viewed through an interface designed  
2415 specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext,  
2416 the TSS shall describe how they are protected/obscured.

## 2417 6.9.3 FPT\_STM.1 Reliable time stamps

2418 (for O.AUDIT)

2419 Hierarchical to: No other components.

2420 Dependencies: No dependencies.

2421 **FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps.

### 2422 **Application note:**

2423 *The time may be set by a trusted administrator or by a network service (e.g., NTP) from a trusted External*  
2424 *IT Entity.*

### 2425 **Assurance Activity:**

2426 TSS:

2427 The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.

2428 Operational Guidance:

2429 The evaluator shall check to ensure that the guidance describes the method of setting the time.

2430 *Test:*

2431 The evaluator shall also perform the following tests:

2432 1. The evaluator shall check to ensure that the time is correctly set up in accordance with the  
2433 guidance or external network services (e.g., NTP).

2434 2. The evaluator shall check to ensure that the time stamps are appropriately provided.

#### 2435 6.9.4 FPT\_TST\_EXT.1 Extended: TSF testing

2436 (for O.TSF\_SELF\_TEST)

2437 Hierarchical to: No other components.

2438 Dependencies: No dependencies.

2439 **FPT\_TST\_EXT.1.1** The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the  
2440 correct operation of the TSF.

#### 2441 **Application note:**

2442 *Power-on self-tests may take place before the TSF is operational, in which case this SFR can be satisfied by*  
2443 *verifying the TSF image by digital signature as specified in FCS\_COP.1(b), or by hash specified in*  
2444 *FCS\_COP.1(c).*

#### 2445 **Assurance Activity:**

2446 TSS:

2447 The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-  
2448 up; this description should include an outline of what the tests are actually doing (e.g., rather than saying  
2449 "memory is tested", a description similar to "memory is tested by writing a value to each memory location  
2450 and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure  
2451 that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating  
2452 correctly.

#### 2453 *Operational Guidance:*

2454 The evaluator shall also ensure that the operational guidance describes the possible errors that may result  
2455 from such tests, and actions the administrator should take in response; these possible errors shall  
2456 correspond to those described in the TSS.

#### 2457 6.9.5 FPT\_TUD\_EXT.1 Extended: Trusted Update

2458 (for O.UPDATE\_VERIFICATION)

2459 Hierarchical to: No other components.

2460 Dependencies: [FCS\_COP.1(b) Cryptographic Operation (for signature generation/verification), or  
2461 FCS\_COP.1(c) Cryptographic Operation (Hash Algorithm)].

2462 **FPT\_TUD\_EXT.1.1** The TSF shall provide authorized administrators the ability to query the current version of the  
2463 TOE firmware/software.

2464 **FPT\_TUD\_EXT.1.2** The TSF shall provide authorized administrators the ability to initiate updates to TOE  
2465 firmware/software.

2466 **FPT\_TUD\_EXT.1.3** The TSF shall provide a means to verify firmware/software updates to the TOE using a digital  
2467 signature mechanism and [***no other functions***] prior to installing those updates.

2468 **Application note:**

2469 *FPT\_TUD\_EXT.1.2 may be interpreted to allow an administrator to “pre-authorize” automatic updates,*  
2470 *provided that they are verified according to FPT\_TUD\_EXT.1.3.*

2471 *The digital signature mechanism is specified in FCS\_COP.1(b). The published hash is generated by one of*  
2472 *the functions specified in FCS\_COP.1(c). It is acceptable to implement both mechanisms.*

2473 **Assurance Activity:**

2474 *TSS:*

2475 The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software  
2476 for update when performing updates, which is consistent with the definition of the SFR.

2477 The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the  
2478 current version of the TOE as well as interfaces to perform updates.

2479 *Operational Guidance:*

2480 The evaluator shall check to ensure that the administrator guidance contains descriptions of the  
2481 operation methods to obtain the TOE version as well as the operation methods to start update  
2482 processing, which are consistent with the description of the TSS.

2483 *Test:*

2484 The evaluator shall also perform the following tests:

- 2485 1. The evaluator shall check to ensure the current version of the TOE can be appropriately obtained by  
2486 means of the operation methods specified by the administrator guidance.
- 2487 2. The evaluator shall check to ensure that the verification of the data for updates of the TOE succeeds  
2488 using authorized data for updates by means of the operation methods specified by the administrator  
2489 guidance.
- 2490 3. The evaluator shall check to ensure that only administrators can implement the application for  
2491 updates using authorized data for updates.
- 2492 4. The evaluator shall check to ensure that the updates are correctly performed by obtaining the current  
2493 version of the TOE after the normal updates finish.
- 2494 5. The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using  
2495 unauthorized data for updates by means of the operation methods specified by the administrator  
2496 guidance. (The evaluator shall also check those cases where hash verification mechanism and digital  
2497 signature verification mechanism fail.)

2498 **6.10 Class FRU: Resource Utilization**

2499 There are no class FRU requirements.

2500 **6.11 Class FTA: TOE Access**

2501 **6.11.1 FTA\_SSL.3 TSF-initiated termination**

2502 (for O.USER\_I&A)

2503 Hierarchical to: No other components.

2504 Dependencies: No dependencies.

2505 **FTA\_SSL.3.1** The TSF shall terminate an interactive session after a [*lapse of Operation Panel auto logout time, lapse of WIM auto logout time, completion of document data reception from the printer driver, and completion of document data reception from the fax driver*].

2508 **Assurance Activity:**

2509 *TSS:*

2510 The evaluator shall check to ensure that the TSS describes the types of user sessions to be terminated  
2511 (e.g., user sessions via operation panel or Web interfaces) after a specified period of user inactivity.

2512 *Operational Guidance:*

2513 The evaluator shall check to ensure that the guidance describes the default time interval and, if it is  
2514 settable, the method of setting the time intervals until the termination of the session.

2515 *Test:*

2516 The evaluator shall also perform the following tests:

- 2517 1. If it is settable, the evaluator shall check to ensure that the time until the termination of the  
2518 session can be set up by the method of setting specified in the administrator guidance.
- 2519 2. The evaluator shall check to ensure that the session terminates after the specified time interval.
- 2520 3. The evaluator shall perform the tests 1 and 2 described above for all the user sessions identified  
2521 in the TSS.

2522 **6.12 Class FTP: Trusted Paths/Channels**

2523 **6.12.1 FTP\_ITC.1[IPsec] Inter-TSF trusted channel**

2524 (for O.COMMS\_PROTECTION, O.AUDIT)

2525 Hierarchical to: No other components.

2526 Dependencies: [FCS\_IPSEC\_EXT.1 Extended: IPsec selected, or  
2527 FCS\_TLS\_EXT.1 Extended: TLS selected, or  
2528 FCS\_SSH\_EXT.1 Extended: SSH selected, or  
2529 FCS\_HTTPS\_EXT.1 Extended: HTTPS selected].

2530 **FTP\_ITC.1.1[IPsec] Refinement:** The TSF shall use [*IPsec*] to provide a **trusted** communication channel between  
2531 itself and **authorized IT entities supporting the following capabilities: [LDAP, FTP, NTP, syslog, and SMTP]** that  
2532 is logically distinct from other communication channels and provides assured identification of its end points and  
2533 protection of the channel data from **disclosure and detection of modification of the channel data**.

2534 **FTP\_ITC.1.2[IPsec] Refinement:** The TSF shall permit **the TSF, or the authorized IT entities,** to initiate  
2535 communication via the trusted channel

2536 **FTP\_ITC.1.3[IPsec] Refinement:** The TSF shall initiate communication via the trusted channel for  
2537 [**communication via the LAN of document data, function data, protected data, and confidential data**].

2538 **Application note:**

2539 *The assignment in FTP\_ITC.1.3 should address the confidentiality and/or integrity requirements for*  
2540 *communication of User and TSF Data between the TOE and another IT entity. FTP\_TRP.1 is intended to be*  
2541 *used for interactive communication between the TOE and remote users.*

2542 *The intent of the above requirement is to use a cryptographic protocol to protect external communications*  
2543 *with authorized IT entities that the TOE interacts with to perform its functions. Protection (by one of the*  
2544 *listed protocols) is required at least for communications with the server that collects the audit information.*  
2545 *If it communicates with an authentication server (e.g., RADIUS), then the ST author chooses*  
2546 *“authentication server” in FTP\_ITC.1.1 and this connection must be protected by one of the listed*  
2547 *protocols. If other authorized IT entities (e.g., NTP server) are protected, the ST author makes the*  
2548 *appropriate assignments (for those entities) and selections (for the protocols that are used to protect*  
2549 *those connections). After the ST author has made the selections, they are to select the detailed*  
2550 *requirements in Appendix D.2 of HCD PP v1.0 corresponding to their protocol selection to put in the ST. To*  
2551 *summarize, the connection to an external audit collection server is required to be protected by one of the*  
2552 *listed protocols. If an External Authentication server is supported, then it is required to protect that*  
2553 *connection with one of the listed protocols. For any other external server, external communications are not*  
2554 *required to be protected, but if protection is claimed, then it must be protected with one of the identified*  
2555 *protocols.*

2556 *While there are no requirements on the party initiating the communication, the ST author lists in the*  
2557 *assignment for FTP\_ITC.1.3 the services for which the TOE can initiate the communication with the*  
2558 *authorized IT entity.*

2559 *The requirement implies that not only are communications protected when they are initially established,*  
2560 *but also on resumption after an outage. It may be the case that some part of the TOE setup involves*  
2561 *manually setting up tunnels to protect other communication, and if after an outage the TOE attempts to*  
2562 *re-establish the communication automatically with (the necessary) manual intervention, there may be a*  
2563 *window created where an attacker might be able to gain critical information or compromise a connection.*

2564 **Assurance Activity:**

2565 **TSS:**

2566 The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities  
2567 identified in the requirement, each communications mechanism is identified in terms of the allowed  
2568 protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are  
2569 specified and included in the requirements in the ST. The evaluator shall confirm that the operational  
2570 guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and  
2571 that it contains recovery instructions should a connection be unintentionally broken.

2572 **Test:**

- 2573 The evaluator shall also perform the following tests:
- 2574 1. The evaluators shall ensure that communications using each protocol with each authorized IT entity is  
2575 tested during the course of the evaluation, setting up the connections as described in the operational  
2576 guidance and ensuring that communication is successful.
  - 2577 2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow  
2578 the operational guidance to ensure that in fact the communication channel can be initiated from the  
2579 TOE.
  - 2580 3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel  
2581 data are not sent in plaintext.
  - 2582 4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during  
2583 test 1, the connection is physically interrupted. The evaluator shall ensure that when physical  
2584 connectivity is restored, communications are appropriately protected.

2585 Further assurance activities are associated with the specific protocols.

#### 2586 6.12.2 FTP\_TRP.1(a) Trusted path (for Administrators)

2587 (for O.COMMS\_PROTECTION)

2588 Hierarchical to: No other components.

2589 Dependencies: [FCS\_IPSEC\_EXT.1 Extended: IPsec selected, or  
2590 FCS\_TLS\_EXT.1 Extended: TLS selected, or  
2591 FCS\_SSH\_EXT.1 Extended: SSH selected, or  
2592 FCS\_HTTPS\_EXT.1 Extended: HTTPS selected].

2593 **FTP\_TRP.1.1(a) Refinement:** The TSF shall use **[TLS/HTTPS]** to provide a **trusted** communication path between  
2594 itself and **remote administrators** that is logically distinct from other communication paths and provides  
2595 assured identification of its end points and protection of the communicated data from **disclosure and**  
2596 **detection of modification of the communicated data.**

2597 **FTP\_TRP.1.2(a) Refinement:** The TSF shall permit **remote administrators** to initiate communication via the  
2598 trusted path

2599 **FTP\_TRP.1.3(a) Refinement:** The TSF shall require the use of the trusted path for **initial administrator**  
2600 **authentication and all remote administration actions.**

#### 2601 **Application Note:**

2602 *This requirement ensures that authorized remote administrators initiate all communication with the TOE*  
2603 *via a trusted path, and that all communications with the TOE by remote administrators is performed over*  
2604 *this path. The data passed in this trusted communication path are encrypted as defined the protocol*  
2605 *chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE,*  
2606 *and then ensures the detailed requirements in Appendix D.2 of HCD PP v1.0 corresponding to their*  
2607 *selection are copied to the ST if not already present.*

#### 2608 **Assurance Activity:**



2609 TSS:

2610 The evaluator shall examine the TSS to determine that the methods of remote TOE administration are  
2611 indicated, along with how those communications are protected. The evaluator shall also confirm that all  
2612 protocols listed in the TSS in support of TOE administration are consistent with those specified in the  
2613 requirement, and are included in the requirements in the ST.

2614 *Operational Guidance:*

2615 The evaluator shall confirm that the operational guidance contains instructions for establishing the  
2616 remote administrative sessions for each supported method.

2617 *Test:*

2618 The evaluator shall also perform the following tests:

- 2619 1. The evaluators shall ensure that communications using each specified (in the operational guidance)  
2620 remote administration method is tested during the course of the evaluation, setting up the  
2621 connections as described in the operational guidance and ensuring that communication is successful.
- 2622 2. For each method of remote administration supported, the evaluator shall follow the operational  
2623 guidance to ensure that there is no available interface that can be used by a remote user to establish  
2624 a remote administrative sessions without invoking the trusted path.
- 2625 3. The evaluator shall ensure, for each method of remote administration, the channel data are not sent  
2626 in plaintext.

2627 Further assurance activities are associated with the specific protocols.

### 2628 6.12.3 FTP\_TRP.1(b) Trusted path (for Non-administrators)

2629 (for O.COMMS\_PROTECTION)

2630 Hierarchical to: No other components.

2631 Dependencies: [FCS\_IPSEC\_EXT.1 Extended: IPsec selected, or

2632 FCS\_TLS\_EXT.1 Extended: TLS selected, or

2633 FCS\_SSH\_EXT.1 Extended: SSH selected, or

2634 FCS\_HTTPS\_EXT.1 Extended: HTTPS selected].

2635 **FTP\_TRP.1.1(b) Refinement:** The TSF shall use **[TLS/HTTPS]** to provide a **trusted** communication path between  
2636 itself and **remote** users that is logically distinct from other communication paths and provides assured  
2637 identification of its end points and protection of the communicated data from **disclosure and detection of**  
2638 **modification of the communicated data.**

2639 **FTP\_TRP.1.2(b) Refinement:** The TSF shall permit **[the TSF, remote users]** to initiate communication via the  
2640 trusted path

2641 **FTP\_TRP.1.3(b) Refinement:** The TSF shall require the use of the trusted path for **initial user authentication and**  
2642 **all remote user actions.**

2643 **Application Note:**



2644 *This requirement ensures that authorized remote users initiate all communication with the TOE via a*  
2645 *trusted path, and that all communications with the TOE by remote users is performed over this path. The*  
2646 *data passed in this trusted communication path are encrypted as defined the protocol chosen in the first*  
2647 *selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures*  
2648 *the detailed requirements in Appendix D.2 of HCD PP v1.0 corresponding to their selection are copied to*  
2649 *the ST if not already present.*

2650 **Assurance Activity:**

2651 TSS:

2652 The evaluator shall examine the TSS to determine that the methods of remote TOE access for non-  
2653 administrative users are indicated, along with how those communications are protected.

2654 The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE access are  
2655 consistent with those specified in the requirement, and are included in the requirements in the ST.

2656 **Operational Guidance:**

2657 The evaluator shall confirm that the operational guidance contains instructions for establishing the  
2658 remote user sessions for each supported method.

2659 **Test:**

2660 The evaluator shall also perform the following tests:

- 2661 1. The evaluators shall ensure that communications using each specified (in the operational guidance)  
2662 remote user access method is tested during the course of the evaluation, setting up the connections  
2663 as described in the operational guidance and ensuring that communication is successful.
- 2664 2. For each method of remote access supported, the evaluator shall follow the operational guidance to  
2665 ensure that there is no available interface that can be used by a remote user to establish a remote  
2666 user session without invoking the trusted path.
- 2667 3. The evaluator shall ensure, for each method of remote user access, the channel data are not sent in  
2668 plaintext.

2669 Further assurance activities are associated with the specific protocols.

2670

## 7 Security Assurance Requirements (APE\_REQ)

This section describes Security Assurance Requirements (SARs) in the evaluations performed by the evaluator based on the CC. These are all common to the Security Functional Requirements (SFRs) in Section 5. Assurance activities to the individual SFRs are described in their respective sections.

After the ST has been approved for evaluation, the Common Criteria IT Security Evaluation Facilities (ITSEF) will obtain the TOE, necessary IT environment, and the TOE guidance documents. The assurance activities described in the ST (which will be refined by the ITSEF to be TOE-specific, either within the ST or in a separate document) will be performed by the ITSEF. Although these activities were performed under the control of the ITSEF, it is allowed to obtain supports from the developer as well. The results of these activities will be documented and presented (along with the administrative guidance used) for validation.

For each assurance family, “Developer Notes” are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer.

The TOE security assurance requirements specified in Table 28 provides evaluative activities required to address the threats identified in Section 0 of this PP.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

Table 28 TOE Security Assurance Requirements

### 7.1 Class ASE: Security Target evaluation

The ST is evaluated as per ASE activities defined in the CEM. In addition, there may be Assurance Activities specified within the PP that call necessary descriptions to be included in the TSS that are specific to the TOE technology type.

Appendix E of HCD PP v1.0 provides a description of the information expected to be provided regarding the quality of entropy in the random bit generator.

Given the criticality of the key management scheme, this PP requires the developer to provide a detailed description of their key management implementation. This information can be submitted as an appendix to the ST and marked proprietary, as this level of detailed information is not expected to be made publicly available. See Appendix F of HCD PP v1.0 for details on the expectation of the developer’s Key Management Description.

### 7.2 Class ADV: Development

For TOEs conforming to this PP, the information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST. While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities contained in Section 5 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

2703 **7.2.1 ADV\_FSP.1 Basic functional specification**

2704 The functional specification describes the TSF Interfaces (TSFIs). At the level of assurance provided by this PP, it  
2705 is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs  
2706 conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly  
2707 invocable by TOE users (to include administrative users), at this assurance level there is little point specifying  
2708 that such interfaces be described in and of themselves since only indirect testing of such interfaces may be  
2709 possible. The activities for this family for this PP should focus on understanding the interfaces presented in the  
2710 TSS in response to the functional requirements, and the interfaces presented in the AGD documentation. No  
2711 additional “functional specification” document should be necessary to satisfy the assurance activities specified.  
2712 The interfaces that need to be evaluated are characterized through the information needed to perform the  
2713 assurance activities listed, rather than as an independent, abstract list.

**Developer action elements:**

ADV\_FSP.1.1D The developer shall provide a functional specification.

ADV\_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Developer Note: The developer shall provide appropriate TSS description and guidance documents as the functional specification. The TSS description identifies TSFIs associated with each SFR in order to confirm the validity of interface design. The developer is required to provide a description at least at a confirmable level in which TSS description and contents of guidance documents are consistent with each other. In case of insufficient information for evaluation in TSS description and contents of guidance documents, additional documentation can be requested. For the SFRs that cannot be directly operated/confirmed from external interfaces, the developer may be requested to provide additional information.

**Content and presentation elements:**

ADV\_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV\_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV\_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV\_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

**Evaluator action elements:**

ADV\_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV\_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

2714 **Assurance activity:**

2715 TSS:

2716 The evaluator shall confirm identifiable external interfaces from guidance documents and examine that  
2717 TSS description identifies all the interfaces required for realizing SFR.

2718 The evaluator shall confirm identification information of the TSFI associated with the SFR described in the  
2719 TSS and confirm the consistency with the description related to each interface.

2720 The evaluator shall check to ensure that the SFR defined in the ST is appropriately realized, based on  
2721 identification information of the TSFI in the TSS description as well as on the information of purposes,  
2722 methods of use, and parameters for each TSFI in the guidance documents

2723 The assurance activities specific to each SFR are described in Section 5 and the evaluator shall perform  
2724 evaluations by adding to this assurance component.

### 2725 7.3 Class AGD: Guidance Documents

2726 The guidance documents will be provided with the developer's security target. Guidance must include a  
2727 description of how the administrator verifies that the Operational Environment can fulfill its role for the security  
2728 functionality. The documentation should be in an informal style and readable by an administrator.

2729 Guidance must be provided for every Operational Environment that the product supports as claimed in the ST.  
2730 This guidance includes

- 2731 • instructions to successfully install the TOE in that environment; and
- 2732 • instructions to manage the security of the TOE as a product and as a component of the larger  
2733 Operational environment.

2734 Guidance pertaining to particular security functionality is also provided; requirements on such guidance are  
2735 contained in the assurance activities specified in Section 5.

#### 2736 7.3.1 AGD\_OPE.1 Operational user guidance

##### **Developer action elements:**

AGD\_OPE.1.1D The developer shall provide operational user guidance.

Developer Note: The developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

##### **Content and presentation elements:**

AGD\_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD\_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD\_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD\_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

- AGD\_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.
- AGD\_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
- AGD\_OPE.1.7C The operational user guidance shall be clear and reasonable.

**Evaluator action elements:**

- AGD\_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2737 **Assurance activity:**

2738 *Operational Guidance:*

2739 The contents of operational guidance are confirmed by the assurance activities in Section 5 and the TOE  
2740 evaluation in accordance with the CEM.

2741 The evaluator shall check to ensure that the following guidance is provided:

2742 Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the  
2743 transition from the maintenance mode to the normal Operational Environment.

2744 **Application note:**

2745 *During evaluation, the TOE returns to its evaluation configuration. In the field, the TOE may return to the*  
2746 *configuration that was in force prior to entering maintenance mode.*

2747 **7.3.2 AGD\_PRE.1 Preparative procedures**

**Developer action elements:**

- AGD\_PRE.1.1D The developer shall provide the TOE, including its preparative procedures.  
Developer Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.

**Content and presentation elements:**

- AGD\_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
- AGD\_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

**Evaluator action elements:**

- AGD\_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- AGD\_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

2748 **7.4 Class ALC: Life-cycle Support**

2749 At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible  
2750 aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration  
2751 management process. This is not meant to diminish the critical role that a developer's practices play in  
2752 contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made  
2753 available for evaluation at this assurance level.

2754 **7.4.1 ALC\_CMC.1 Labelling of the TOE**

2755 This component is targeted at identifying the TOE such that it can be distinguished from other products or  
2756 version from the same vendor and can be easily specified when being procured by an end user.

**Developer action elements:**

ALC\_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

**Content and presentation elements:**

ALC\_CMC.1.1C The TOE shall be labeled with its unique reference.

**Evaluator action elements:**

ALC\_CMC.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

2757 **Assurance activity:**

2758 *Operational Guidance:*

2759 The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version  
2760 number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall  
2761 ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the  
2762 appropriate administrative guidance) as specified in the ST. Further, the evaluator shall check the AGD  
2763 guidance and TOE samples received for testing to ensure that the version number is consistent with that  
2764 in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the  
2765 information on the web site to ensure that the information in the ST is sufficient to distinguish the  
2766 product.

2767 **7.4.2 ALC\_CMS.1 TOE CM coverage**

2768 Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance  
2769 activities are covered by the assurance activities listed for ALC\_CMC.1.

**Developer action elements:**

ALC\_CMS.1.1D The developer shall provide a configuration list for the TOE.

**Content and presentation elements:**

ALC\_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC\_CMS.1.2C The configuration list shall uniquely identify the configuration items.

**Evaluator action elements:**

ALC\_CMS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

2770 **Assurance activity:**

2771 *Operational Guidance:*

2772 The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled  
2773 with the guidance provided to administrators and users under the AGD requirements. By ensuring that  
2774 the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance  
2775 (as done in the assurance activity for ALC\_CMC.1), the evaluator implicitly confirms the information  
2776 required by this component.

## 2777 7.5 Class ATE: Tests

2778 Testing is specified for functional aspects of the system as well as aspects that take advantage of design or  
2779 implementation weaknesses. The former is done through ATE\_IND family, while the latter is through the  
2780 AVA\_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and  
2781 interfaces as constrained by the availability of design information presented in the TSS. One of the primary  
2782 outputs of the evaluation process is the test report as specified in the following requirements.

### 2783 7.5.1 ATE\_IND.1 Independent testing - Conformance

2784 Testing is performed to confirm the functionality described in the TSS as well as the administrative (including  
2785 configuration and operation) documentation provided. The focus of the testing is to confirm that the  
2786 requirements specified in Section 5 are being met, although some additional testing is specified for SARs in  
2787 Section 7. The Assurance Activities identify the minimum testing activities associated with these components.  
2788 The evaluator produces a test report documenting the plan for and results of testing, as well as coverage  
2789 arguments focused on the product models combinations that are claiming conformance to this PP.

#### **Developer action elements:**

ATE\_IND.1.1D The developer shall provide the TOE for testing.

#### **Content and presentation elements:**

ATE\_IND.1.1C The TOE shall be suitable for testing.

#### **Evaluator action elements:**

ATE\_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for  
content and presentation of evidence.

ATE\_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

2790 **Assurance activity:**

2791 *Test:*

2792 The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test  
2793 plan covers all of the testing actions contained in the body of this PP’s Assurance Activities. While it is not  
2794 necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in  
2795 the test plan that each applicable testing requirement in the ST is covered.

2796 The Test Plan identifies the product models to be tested, and for those product models not included in  
2797 the test plan but included in the ST, the test plan provides a justification for not testing the models. This  
2798 justification must address the differences between the tested models and the untested models, and make  
2799 an argument that the differences do not affect the testing to be performed. It is not sufficient to merely  
2800 assert that the differences have no affect; rationale must be provided. In case the ST describes multiple  
2801 models (product names) in particular, the evaluator shall consider the differences in language



2802 specification as well as the influences, in which functions except security functions such as a printing  
2803 function, may affect security functions when creating this justification. If all product models claimed in the  
2804 ST are tested, then no rationale is necessary.

2805 The test plan describes the composition of each product model to be tested, and any setup that is  
2806 necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators  
2807 are expected to follow the AGD documentation for installation and setup of each model either as part of a  
2808 test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or  
2809 tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the  
2810 performance of the functionality by the TOE.

2811 The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve  
2812 those objectives. These procedures include the goal of the particular procedure, the test steps used to  
2813 achieve the goal, and the expected results. The test report (which could just be an annotated version of  
2814 the test plan) details the activities that took place when the test procedures were executed, and includes  
2815 the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in  
2816 a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass”  
2817 result (and the supporting details), and not just the “pass” result.

## 2818 7.6 Class AVA: Vulnerability Assessment

2819 For the first generation of this protection profile, the evaluation lab is expected to survey open sources to  
2820 discover what vulnerabilities have been discovered in these types of products. In most cases, these  
2821 vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and  
2822 uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in  
2823 the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the  
2824 documentation provided by the vendor. This information will be used in the development of penetration testing  
2825 tools and for the development of future protection profiles.

### **Developer action elements:**

AVA\_VAN.1.1D The developer shall provide the TOE for testing.

### **Content and presentation elements:**

AVA\_VAN.1.1C The TOE shall be suitable for testing.

### **Evaluator action elements:**

AVA\_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA\_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA\_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing basic attack potential.

### 2826 **Assurance activity:**

2827 *Test:*

2828 As with ATE\_IND, the evaluator shall generate a report to document their findings with respect to this  
2829 requirement. This report could physically be part of the overall test report mentioned in ATE\_IND, or a



2830 separate document. The evaluator performs a search of public information to determine the  
2831 vulnerabilities that have been found in printing devices and the implemented communication protocols in  
2832 general, as well as those that pertain to the particular TOE. The evaluator documents the sources  
2833 consulted and the vulnerabilities found in the report.

2834 For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability,  
2835 or the evaluator formulates a test (using the guidelines provided in ATE\_IND) to confirm the vulnerability,  
2836 if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the  
2837 vulnerability.

2838 For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example,  
2839 a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an  
2840 electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an  
2841 appropriate justification would be formulated.

#### 2842 [7.7 Security Assurance Requirements rationale](#)

2843 The rationale for choosing these security assurance requirements is that they define a minimum security  
2844 baseline that is based on the anticipated threat level of the attacker, the security of the Operational  
2845 Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities  
2846 throughout the PP are used to provide tailored guidance on the specific expectations for completing the security  
2847 assurance requirements.

## 2848 8 TOE Summary Specification (ASE\_TSS)

2849 This section provides a summary specification for each TOE security function. The security functions are  
2850 described for each corresponding security functional requirement.

### 2851 8.1 Identification and Authentication, Use-of-Feature Authorization (TSF\_FIA)

2852 The Identification and Authentication Function verifies that users are authorized to operate the TOE and access  
2853 the TOE's protected information.

#### 2854 8.1.1 FIA\_UAU.1 and FIA\_UID.1

2855 The TOE identifies and authenticates a user by checking credentials entered by the user.

2856 User credentials are checked against user authentication data stored in the TOE, or against an external network  
2857 authentication service (LDAP).

2858 Users can be identified and authenticated through several interfaces:

- 2859 • Locally, manually entering a username and password using the Operation Panel.
- 2860 • Remotely, manually entering credentials using a client computer's web browser to access the Web  
2861 Image Monitor (WIM).
- 2862 • Remotely, using a client computer's print driver or fax driver which has been configured to submit  
2863 credentials on behalf of the user.

2864 When users are identified and authenticated via remote interfaces, their credentials are protected in transit  
2865 using trusted paths.

2866 Certain functions may be performed without user identification and authentication:

- 2867 • Viewing user job lists, WIM Help, system status, the counter and information of inquiries, repair request  
2868 notifications, and eco information of system.
- 2869 • Creation of fax reception jobs.
- 2870 • Creation of print jobs.

#### 2871 8.1.2 FIA\_PMG\_EXT.1

2872 For authentication within the TOE, login passwords for users can be registered only if these passwords meet the  
2873 conditions specified by the selections in FIA\_PMG\_EXT.1.

#### 2874 8.1.3 FIA\_UAU.7

2875 When users enter their passwords using the Operation Panel or using WIM from the client computer, the TOE  
2876 displays a sequence of dummy characters whose length is the same as that of the entered password.

#### 2877 8.1.4 FIA\_AFL.1

2878 The TOE counts consecutive login failures for a given login name and locks out that user until the lockout is  
2879 released. The TOE can lock out any user.

2880 Authentication events that are subject to lockout are listed with the SFR FIA\_AFL.1.1 in Table 22, and the actions  
2881 to release lockout are listed with the SFR FIA\_AFL.1.2 in Table 23.

2882 **8.1.5 FIA\_USB.1 and FIA\_ATD.1**

2883 After successful identification and authentication, users are authorized to perform functions according to the  
2884 user role (Normal User, MFP Administrator, or MFP Supervisor) that is associated with their user registration.  
2885 The user security attributes associated with each role are:

- 2886 • Login User Name
- 2887 • User Role
- 2888 • Available Functions List

2889 The User Role assigned to the user at login is maintained until the user is logged out. If user identification and  
2890 authentication fails, use of the TOE is denied according to FIA\_UAU.1 and FIA\_UID.1.

2891 An Available Functions List is associated with each Normal User. It lists the basic hardcopy functions that the  
2892 user is permitted to perform.

2893 **8.1.6 FTA\_SSL.3**

2894 User sessions are terminated according to the type of user session:

2895 **Operation Panel:** the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time  
2896 (settable from 10 to 999 seconds).

2897 **WIM:** the user is logged out of the TOE when inactivity reaches the WIM auto logout time (settable from 3 to 60  
2898 minutes).

2899 **Printer driver:** the user is logged out of the TOE immediately after receiving the print data from the printer  
2900 driver.

2901 **Fax driver:** the user is logged out of the TOE immediately after receiving the transmission information from the  
2902 fax driver.

2903 **Network login:** the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time  
2904 (settable from 10 to 999 seconds).

2905 **8.2 Access Control (TSF\_FDP)**

2906 The Access Control Function permits authorized TOE users to operate document data and user jobs in  
2907 accordance with the privileges allowed by their user role.

2908 **8.2.1 FDP\_ACC.1 and FDP\_ACF.1**

2909 The TOE controls user operations for document data and user jobs as specified in Table 20 and Table 21.

2910 *8.2.1.1 Access control rule on document data*

2911 The TOE provides users with the ability to perform operations on document data that are stored in the TOE.

2912 Normal Users are permitted to operate on document data if the ID of the user corresponds to the Document  
2913 User List for that document (i.e., the user is the "Job Owner"). A Normal User is not permitted to operate on  
2914 document data for which it is not the Job Owner. The privileges that allow users to edit the Document User List  
2915 are described in section 8.5.

2916 As described in Table 29, a Normal User who is a Job Owner may print, download to client computers, send by  
2917 fax, send by e-mail as attachments, and delete stored documents, using the Operation Panel or a web browser.

2918 The TOE allows only the Job Owner to view and delete the document data handled as a user job while Copy  
 2919 Function, Printer Function, Scanner Function, Fax Function, or Document Server Function is being used.

2920 While no interface to change job owners is provided, an interface to cancel user jobs is provided. If a user job is  
 2921 cancelled, any document the cancelled job operates will be deleted.

Function	User interface	Type of document	Operations permitted for authorized users
Printer	Operation Panel	+PRT	Print Delete
Printer	Web browser	+PRT	Print Delete
Scanner	Operation Panel	+SCN	E-mail transmission
Fax	Operation Panel	+FAXIN	Print Delete
Fax	Web browser	+FAXIN	Print Download Delete (Operations above are permitted only if Normal Users are authorized to use Document Server Function)
Document Server	Operation Panel	+DSR	Print Delete
Document Server	Operation Panel	+FAXOUT	Print Delete
Document Server	Web browser	+DSR	Print Delete
Document Server	Web browser	+FAXOUT	Fax transmission Download Print Delete (Fax transmission is permitted for Normal Users who are authorized to use Fax Function)

2922 *Table 29 Stored Documents Access Control Rules for Normal Users*

2923 MFP Administrators are not permitted to print, download, or send stored documents. MFP Administrators may  
 2924 delete stored documents, using the Operation Panel, web browser, or indirectly by cancelling a job.

2925 The MFP Supervisor is not permitted to perform any document operations.

2926 *8.2.1.2 Access control rule on user jobs*

2927 The TOE displays on the Operation Panel a menu to cancel a user job only if the user who logs in from the  
 2928 Operation Panel is a Job Owner or MFP Administrator and a cancellation of a user job is attempted by the Job  
 2929 Owner or an MFP Administrator. Other users are not allowed to operate user jobs.

2930 When a user job is cancelled, any documents operated by the cancelled job will be deleted. However, if the  
 2931 document data operated by the cancelled user job is a stored document, the data will not be deleted and  
 2932 remain stored in the TOE.

2933 **8.3 Stored Data Encryption (TSF\_FCS)**

2934 The Stored Data Protection Function encrypts data on the HDD and in NVRAM.

2935 **8.3.1 FCS\_KYC\_EXT.1, FPT\_KYP\_EXT.1, and FCS\_COP.1(f)**

2936 The keychain for encrypting field-replaceable non-volatile storage devices begins with a common Root  
 2937 Encryption Key (REK). The plaintext REK is stored in a hardware security module, Ic Key.

2938 The REK is used to encrypt and decrypt a Key Encryption Key (KEK). The KEK is used to encrypt and decrypt  
 2939 Device Encryption Keys (DEKs) for the HDD and NVRAM. All such operations use 256-bit AES keys to protect 256-  
 2940 bit AES data encryption on the target devices.

Key	En/decrypts	Algorithm	Length	SFR	Validation
Root Encryption Key (REK)	Key Encryption Key	AES CBC	256	FCS_COP.1(f)	CAVP AES #5364
Key Encryption Key (KEK)	HDD Key NVRAM Key DevCert Key	AES CBC	256	FCS_COP.1(f)	CAVP AES #5364

2941 *Table 30 Keychain encryption*

2942 Additional details about the keychain and device encryption are provided in the Key Management Description.

2943 **8.3.2 FCS\_CKM.1(b)[DIM], FCS\_CKM.1(b)[DAR], and FCS\_RBG\_EXT.1**

2944 The REK, KEK, HDD Key, and NVRAM Key, are created using a software-based DRBG that has been seeded by a  
 2945 third-party hardware-based TRNG and DRBG.

RNG	Method	Standard	Validation
Hardware TRNG	True RNG + DRBG	AIS31 Class 2	CC #ANSSI-CC-2012/84
Software DRBG	Hash_DRBG_SHA256	SP 800-90A	CAVP HMAC #3552 CAVP SHS #4306 CAVP DRBG #2075

2946 *Table 31 Random Number Sources*

2947 Additional details about key creation, the TRNG, and the DRBG, are provided in the Key Management  
 2948 Description and Entropy Description documents.

2949 **8.3.3 FCS\_CKM.4 and FCS\_CKM\_EXT.4**

2950 Key destruction details are provided in the Key Management Description.

2951 **8.3.4 FDP\_DSK\_EXT.1 and FCS\_COP.1(d)**

2952 Two field-replaceable non-volatile storage devices employ encryption: the HDD, and NVRAM.

2953 The entire HDD is encrypted. All HDD data is encrypted with AES 256 CBC encryption by a hardware component,  
 2954 Ic Ctrl. HDD encryption is enabled and initialized in the evaluated configuration, as described in the Notes for  
 2955 Administrators guidance document.

2956 Partition 3 of NVRAM is encrypted a software component, LPUX NVRAM Encryption Driver, with AES 256-bit  
 2957 encryption. It is enabled and initialized during manufacturing and cannot be disabled. Other partitions of  
 2958 NVRAM do not contain confidential User or TSF Data.

2959 The following algorithms are used:

Function	SFR	Algorithm	Validation
HDD encryption	FCS_COP.1(d)	AES 256 CBC	AES #3921
NVRAM encryption	FCS_COP.1(d)	AES 256 CBC	AES #4560

2960 *Table 32 Storage encryption cryptographic functions*

2961 Keychain, key management, and other details are provided in the Key Management Description.

2962 **8.4 Trusted Communications (TSF\_FTP)**

2963 The Trusted Communications Function provides trusted paths for communications between the TOE and remote  
 2964 users / external IT entities.

2965 **8.4.1 FTP\_TRP.1 (a), FTP\_TRP.1 (b), FCS\_HTTPS\_EXT.1, and FCS\_TLS\_EXT.1**

2966 The TOE employs TLS 1.2 to protect communications between the TOE and remote users' client computers  
 2967 (print drivers, fax drivers, and WIM HTTPS sessions).

2968 The TOE supports these ciphersuites:

- 2969 • TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- 2970 • TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- 2971 • TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 2972 • TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- 2973 • TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 2974 • TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- 2975 • TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- 2976 • TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

2977 **8.4.2 FCS\_CKM.1 (a), FCS\_RBG\_EXT.1, FCS\_COP.1 (a), FCS\_COP.1(b)[DIM], FCS\_COP.1(c) , and**  
 2978 **FCS\_COP.1(g)**

2979 The TOE generates a self-signed Device Certificate according to FCS\_CKM.1(a). Administrators may import a  
 2980 Device Certificate that is generated outside of the TOE.

2981 To establish a session key for TLS communications, the TOE employs a Diffie-Hellman-based key establishment  
 2982 scheme conforming to NIST SP 800-56A, and a Hash DRBG. The session key is used to encrypt communications  
 2983 with AES 128 or AES 256 CBC:

Function	SFR	Algorithm	Validation
Key establishment	FCS_CKM.1(a)	DSA KeyGen 186-4	DSA #1385
	FCS_COP.1(b)[DIM]	KAS-FFC	Comp #1826
	FCS_COP.1(c)		
Random number generation	FCS_RBG_EXT.1	Hash_DRBG_SHA256	HMAC #3552 DRBG #2075 SHS #4306
Encryption / decryption	FCS_COP.1(a)	AES 128 CBC AES 256 CBC	AES #5364

2984 *Table 33 TLS/HTTPS cryptographic functions*

2985 Per IG D.8, Scenario 6 – non-approved primitive only, a partial DH key agreement scheme is allowed in an  
 2986 approved FIPS mode of operation. No keys are established into the module using DH. Key establishment  
 2987 methodology provides 112 bits of encryption strength.

2988 **8.4.3 FPT\_SKP\_EXT.1, FCS\_CKM.4 and FCS\_CKM\_EXT.4**

2989 All pre-shared keys, symmetric keys, and private keys are protected in storage and are not accessible to any user  
 2990 through TOE interfaces. A root encryption key is securely stored in IcKey (a Trusted Platform Module). No other  
 2991 plaintext keys are stored in non-volatile storage. The root encryption key is used to decrypt a key encryption key

2992 which is used to decrypt symmetric keys for encrypted storage and the Device Certificate. The IPsec PSK is  
 2993 stored in an encrypted partition of NVRAM. Key destruction is described in the Key Management Description.

2994 **8.4.4 FCS\_ITC.1[IPsec], FCS\_IPSEC\_EXT.1, FIA\_PSK\_EXT.1, and FCS\_COP.1(g)**

2995 The TOE employs IPsec to protect communications between the TOE and external IT entities in the operational  
 2996 environment. In the evaluated configuration, it is used for communications with LDAP, syslog, NTP, SMTP, and  
 2997 FTP servers.

2998 IPsec is operated in transport mode, as set by the administrator.

2999 IPsec supports automatic key exchange or automatic key exchange by IKEv1.

3000 In Phase 1, peer authentication supports two types of authentication: pre-shared key authentication and digital  
 3001 certificate authentication.

3002 The pre-shared key can be any length from 1 to 32 characters, and composed of any combination of upper and  
 3003 lower case letters, numbers, and special characters (that include: "!", "@", "#", "\$", "%", "^", "&", "\*", "(", and  
 3004 ")").

3005 An administrator can select whether to use main mode or aggressive mode. In the evaluated configuration, only  
 3006 main mode is used.

3007 In IKEv1, supported DH groups are 1,2 and 14. The value set by the administrator is used.

3008 IKEv1 key lifetimes can be set by the administrator, from 300 seconds to 172,800 seconds. In the evaluated  
 3009 configuration, Phase 1 key lifetime is set to 86,400 seconds (24 hours), and Phase 2 lifetime is set to 28,800  
 3010 seconds (8 hours).

3011 As an SPD, four individual entries and one default entry can be set by an administrator. Beginning with the first  
 3012 entry the packet is compared, and if it matches the entry, IPsec communication is performed. If the packet does  
 3013 not match the first entry, subsequent entries are tested until there is a match. If no entries match the packet,  
 3014 the default entry will be compared, and if it does not match, the packet is discarded.

3015 The TOE supports these cryptographic algorithms:

Function	SFR	Algorithm	Validation
IKEv1	FCS_CKM.1(a)	RSA 186-4	RSA #2869
	FCS_COP.1(a)	AES 128 CBC	AES #5364
	FCS_COP.1(b)[DIM]	AES 256 CBCHMAC-SHA256	HMAC #3552
	FCS_COP.1(g)	HMAC-SHA384	SHS #4306
	FCS_RBG_EXT.1	HMAC-SHA512	
ESP	FCS_COP.1(a)	AES 128 CBC	AES #5315
	FCS_COP.1(b)[DIM]	AES 256 CBC	HMAC #3515
	FCS_COP.1(g)	HMAC-SHA256	SHS #4269
	FCS_COP.1(g)	HMAC-SHA384	
	FCS_RBG_EXT.1	HMAC-SHA512	

3016 *Table 34 IPsec cryptographic functions*



3017 **8.5 Administrative Roles (TSF\_FMT)**

3018 The Security Management Function consists of functions to 1) control operations for TSF data, 2) maintain user  
 3019 roles assigned to Normal Users, MFP Administrator, or MFP Supervisor to operate the Security Management  
 3020 Function, and 3) set appropriate default values to security attributes, all of which accord with user role privileges  
 3021 or user privileges that are assigned to Normal Users, MFP Administrator, or MFP Supervisor.

3022 **8.5.1 FMT\_SMR.1**

3023 The TOE maintains U.NORMAL and U.ADMIN roles as described in Table 6. Normal Users are permitted to use  
 3024 document processing functions TOE and access their own data. Administrators do not initiate document  
 3025 processing jobs: the sub-role MFP Administrator can manage Normal Users' jobs and data and configures the  
 3026 TOE, and the sub-role MFP Supervisor sets MFP Administrators' passwords.

3027 **8.5.2 FMT\_SMF.1, FMT\_MOF.1, and FMT\_MTD.1**

3028 The TOE provides management functions listed in Table 26 and the TOE restricts operations on TSF Data  
 3029 according to the rules described in Table 26.

3030 **8.5.3 FMT\_MSA.1 and FMT\_MSA.3**

3031 The TOE restricts operations on security attributes according to the rules described in Table 25.

3032 The TOE sets default values for objects/subjects according to the rules described in Table 35 when those  
 3033 objects/subjects are generated.

Objects	Security attributes	Default values
Document data	Document data attribute	+PRT: Documents printed from the client computer with direct print, locked print, hold print, and sample print. +SCN: Documents sent by e-mail as attachments from the MFP. +CPY: Documents copied using the MFP. +FAXOUT: Documents sent by fax from the MFP or client computer. +FAXIN: Documents received from a telephone line. +DSR: Documents stored in the TOE by using Copy Function, Scanner Function, Document Server Function and Fax Data Storage Function. Documents printed using Document Server printing or stored print from the client computer.
Document data (stored document types are Document Server document, scanner document and fax transmission document)	Document user list	Default values of a document user list assigned to a Normal User who created the document data.
Document data (stored document type is printer document)	Document user list	Login user name of a Normal User who stored the document data.
Document data (stored document type is fax reception document)	Document user list	Login user name of a Normal User included in the Stored Reception File User list.



Objects	Security attributes	Default values
User jobs	Login user name of Normal User	Login user name of a Normal User who newly creates a user job.
Each MFP application (Copy Function, Printer Function, Scanner Function, Document Server Function and Fax Function)	Function type	The values specified for each function type is as follows: For Copy Function, values to identify Copy Function. For Document Server Function, values to identify Document Server Function. For Printer Function, values to identify Printer Function. For Scanner Function, values to identify Scanner Function. For Fax Function, values to identify Fax Function.

3034 *Table 35 List of Static Initialization for Security Attributes of Document Access Control SFP*

3035 The attributes which may be overridden are restricted to U.ADMIN, as described in Table 36

Object	Attribute	Role that can override default value
Document data when attribute is +DSR or +FAXIN	Document user list	MFP Administrator

3036 *Table 36 Roles allowed to override default values*

3037 **8.6 Audit Function (TSF\_FAU)**

3038 The Audit Function is to generate the audit log of TOE use and security-relevant events (hereafter, "audit events"). This function provides the recorded audit log in a legible fashion for users to audit (audit log review).

3040 The recorded audit log can be accessed and deleted only by the MFP Administrator.

3041 **8.6.1 FAU\_GEN.1 and FAU\_GEN.2**

3042 The TOE records an audit log of events listed in Table 37.

Auditable event requirements	Auditable events satisfied
Start-up and shutdown of the audit functions	Start-up of the Audit Function
	Shutdown of the Audit Function
Job completion	Printing via networks
	LAN Fax via networks
	Scanning documents
	Copying documents
	Receiving incoming faxes
	Creating document data (storing)
	Reading document data (print, download, fax transmission)
	Deleting document data
Unsuccessful User authentication, Unsuccessful User identification	Failure of login operations
Use of management functions	Use of functions identified in FMT_SMF.1
Modification to the group of Users that are part of a role	Modification of MFP Administrator roles
Changes to the time	Date settings (year/month/day), time settings (hour/minute)
Failure to establish session	Failure of communication with the audit server
	Failure of communication with the authentication server
	Failure of communication with the FTP server
	Failure of communication with the NTP server
	Failure of communication with print driver
	Failure of communication with fax driver
	Failure of communication with WIM

3043 *Table 37 List of Audit Events*

3044 Audit log entries record the date and time of the event, type of event, subject identity (if applicable), and the  
3045 outcome (success or failure) of the event. Additionally Job Completion events record the type of job, and Failure  
3046 to Establish Session events record the reason for such failure.

3047 The complete list of audit log items, attributes, and content, can be found in the guidance documentation in  
3048 “Logs That Can Be Managed Using Web Image Monitor”.

#### 3049 [8.6.2 FAU\\_STG.1, FAU\\_STG\\_EXT.1, FAU\\_STG.4, FAU\\_SAR.1, and FAU\\_SAR.2](#)

3050 The TOE stores audit log data in a dedicated storage area of the HDD. Audit records are buffered in that storage  
3051 area before transfer to an audit server or retrieval by an Administrator.

3052 Audit data is Confidential TSF Data. Audit records can be retrieved by:

- 3053 • An Administrator, using the WIM to initiate transfer of audit records.
- 3054 • An Administrator-configured transfer over a trusted channel (IPSec) to the Audit Server in the  
3055 Operational Environment.

3056 Administrator-configuration can initiate transfers on a time schedule, when the log storage area is reaching its  
3057 capacity, or whenever events are logged.

3058 There are three types of audit logs: Job logs, Access logs, and Ecology logs. The maximum number of records  
3059 that can be stored in the TOE are:

- 3060 • Job log: 4,000 records
- 3061 • Access log: 12,000 records
- 3062 • Ecology log: 4,000 records

3063 If a maximum is reached, records are overwritten by new records according to the following order:

- 3064 1. Records that have been transferred and records that are not set for transfer, oldest first
- 3065 2. Records for completed events that are set for transfer but not yet transferred, oldest first
- 3066 3. Records that are in process, oldest first

#### 3067 [8.6.3 FPT\\_STM.1](#)

3068 The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from  
3069 the system clock of the TOE. The system clock is also used for other time-related functions, including user  
3070 lockout timing, idle session timeouts, and SA lifetimes.

3071 The system clock may be set locally or configured to use a network time server. Only an MFP Administrator can  
3072 configure the system clock.

### 3073 [8.7 Trusted Operation \(TSF\\_FPT\)](#)

3074 The Software Verification Function is to verify the integrity of the executable codes of the MFP Control Software,  
3075 FCU Control Software and Operation Panel Control Software, and confirm that these codes can be trusted.

#### 3076 [8.7.1 FPT\\_TST\\_EXT.1, FCS\\_COP.1\(b\), FCS\\_COP.1\(c\)\[L1\], and FCS\\_COP.1\(c\)\[L2\]](#)

3077 During start-up, the TOE verifies the integrity of the TSF through a series of integrity tests, using the  
3078 cryptographic functions listed below.

Integrity test	SFR	Algorithm	Validation
----------------	-----	-----------	------------

TPM	FCS_COP.1(c)[L1]	SHA-1	SHS #C715
MFP Control Software	FCS_COP.1(b) FCS_COP.1(c)[L2]	RSA 186-4 SHA-256	RSA #2002 SHS #3231
Fax Control Unit	FCS_COP.1(c)[L1]	SHA-1	SHS #2363
Operation Panel Software	FCS_COP.1(b) FCS_COP.1(c)[L1]	RSA 186-4 SHA-1	RSA #C582 SHS #C582
Operation Panel Applications	FCS_COP.1(b) FCS_COP.1(c)[L1]	RSA 186-4 SHA-1	RSA # C582 SHS # C582

3079 *Table 38 Start-up integrity tests*

3080 TOE also performs Entropy testing as described in a separate Entropy Description document.

3081

3082 Testing the BIOS, MFP and Operation Panel operating systems, applications, and entropy source, demonstrates  
 3083 that the entire TSF is operating correctly.

3084 If any of these steps fails, the TOE displays a Service Call (SC) error code on the Operator Panel and the TOE  
 3085 becomes unavailable. In such cases, the Administrator should contact a Customer Engineer to service the TOE.

3086 If all steps succeed, then the TOE becomes available.

### 3087 **8.7.2 FPT\_TUD\_EXT.1, FCS\_COP.1(b), FCS\_COP.1(c)[L1], and FCS\_COP.1(c)[L2]**

3088 TOE allows only the MFP Administrator to read the version of the MFP Control Software, Operation Panel  
 3089 Control Software, and FCU Control Software. The MFP Administrator can read these versions using the  
 3090 Operation Panel or WIM from the client computer.

3091 The MFP Administrator can prepare for installation of updated MFP Control Software, Operation Panel Software,  
 3092 or FCU Control Software, by uploading an installation package from the client computer using WIM. The package  
 3093 contains the TOE Software and a digital signature (DS) that was created using the SERES private key. Digital  
 3094 signatures for trusted updates are generated outside of the TOE, by the manufacturer.

3095 For MFP Control or FCU Software, the TOE performs the following verifications before the installing the package:

- 3096 1. Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);
- 3097 2. Verifies that the software model name matches the TOE;
- 3098 3. Creates a SHA256 message digest (MD1) of the software, uses the SERES public key to decrypt DS (MD2),  
 3099 and then verifies that MD1 = MD2.

3100 For Operation Panel software, the TOE performs the following verifications before the installing the package:

- 3101 1. Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);
- 3102 2. Verifies that the software model name matches the TOE;
- 3103 3. Creates a SHA256 message digest (MD1) of the index file, uses the SERES public key to decrypt DS  
 3104 (MD2), and then verifies that MD1 = MD2.
- 3105 4. Creates a SHA256 message digest (MD3) of the software image, uses an internal key to decrypt DS  
 3106 (MD4), and then verifies that MD3 = MD4.

3107 The TOE performs the signature verification of the software to be updated using the encryption functions listed  
 3108 below when updating the software.

Integrity test	SFR	Algorithm	Validation
MFP Control Software	FCS_COP.1(b)	RSA 186-4	RSA #2002
	FCS_COP.1(c)[L2]	SHA-256	SHS #3231
Operation Panel Software	FCS_COP.1(b)	ECDSA SigVar 186-4	ECDSA # C629
	FCS_COP.1(c)[L2]	SHA-256	SHS # C629
Operation Panel Applications	FCS_COP.1(b)	RSA 186-4	RSA # C582
	FCS_COP.1(c)[L2]	ECDSA SigVar 186-4	ECDSA # C582
		SHA-256	SHS # C582

3109

## 3110 8.8 PSTN Fax-Line Separation (TSF\_FXS)

3111 The Fax Line Separation Function permits only fax transmissions as input information from telephone lines so  
 3112 that unauthorized intrusion from telephone lines can be prevented.

### 3113 8.8.1 FDP\_FXS\_EXT.1

3114 The fax interface use cases are below.

- 3115 • Sending faxes
  - 3116 ○ The TOE receives documents from client PCs via the LAN, and using the fax interface, transmits
  - 3117 them as fax documents via the PSTN line using the ITU-T T.30 protocol.
  - 3118 ○ The TOE can transmit stored documents as faxes.
- 3119 • Receiving faxes
  - 3120 ○ A remote fax machine establishes a connection to the TOE through the PSTN line using the ITU-T
  - 3121 T.30 protocol, through which the TOE receives fax documents.
- 3122 • Fax-Line Separation
  - 3123 ○ The fax modem accepts connections through the PSTN only if they conform to the ITU-T T.30
  - 3124 protocol.
  - 3125 ○ Data that is transmitted or received through the PSTN is fax-format, image data.

## 3126 8.9 Image Overwrite

### 3127 8.9.1 FDP\_RIP.1(a)

3128 During the processing of jobs, image data is stored on the HDD. When such data is no longer needed by the user  
 3129 or the TOE, residual data can be overwritten using the Auto Erase Memory function.

3130 When enabled, the Auto Erase Memory function automatically overwrites the residual image data after each  
 3131 completion of the following processing jobs:

- 3132 • Copy jobs

- 3133 • Print jobs
- 3134 • Sample Print/Locked Print/Hold Print
- 3135 • Stored Print jobs (after deletion of the job)
- 3136 • Spool printing jobs
- 3137 • LAN-Fax print data
- 3138 • Faxes sent/received using remote machines
- 3139 • Scanned files sent by e-mail
- 3140 • Files sent by Scan to Folder
- 3141 • Documents sent using Web Image Monitor
- 3142 • Documents deleted from the Document Server using the Copier, Printer, Fax or Scanner functions

3143 When the Auto Erase Memory function is enabled, such data is actively overwritten with values and repetition  
3144 selected by the Administrator:

- 3145 • NSA: Temporary data is overwritten twice with random numbers and once with zeros.
- 3146 • DoD: Each item of data is overwritten by a random number, then by its complement, then by another  
3147 random number, and is then verified.
- 3148 • Random Numbers: Temporary data is overwritten multiple times with random numbers. The number of  
3149 overwrites can be selected from 1 to 9, default 3.

3150

## A Terminology

3151

### A.1 Glossary

Term	Definition	Source
Address Book	Electronic storage mechanism that equates names of persons or physical locations with machine-usable destinations (e.g., fax telephone numbers, email addresses, Uniform Resource Locators).	
Administrator	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the security policies of the TOE. Administrators may possess special privileges that provide capabilities to override portions of security policies.	[2600.1]
Asset	Entities that the owner of the TOE presumably places value upon.	[CC]
Assumption	Physical, technical, and administrative conditions or requirements of the Operational Environment that must be upheld in order for the TOE to provide security functionality.	
Border Encryption Value	A secret value passed to a storage encryption component such as a self-encrypting storage device.	[CPP_FDE_E E_V2.0]
Commercial Off-The-Shelf	Products that are both commercial and sold in substantial quantities in the commercial marketplace, and that can be procured or utilized under government contract in the same precise form as available to the general public.	[FAR]
Confidential (TSF) Data	Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.	[2600.1]
Create	Assigning a value or content to data in a storage device. Note that in the case of document processing jobs, the outcome is that the job is initiated	
Credentials	A form of authentication data that specifies basic identifying information about a User or application. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer Credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.	[2600]
Decommission	The act of retiring an HCD from active use in the Operational Environment. It may also involve a change in geographic location and/or ownership.	
Delete	Dereferencing or otherwise making unavailable data in a storage device. Note that in the case of document processing jobs, the outcome is that the job is terminated.	
Document	A medium and the information recorded on it that generally has permanence and can be read by a person or a machine.	[610.12]
Document Processing	Printing, scanning, or copying a Document.	
Document Processing Job	A User request to the TOE to perform a Document Processing operation on a Document.	
Entropy Description	A non-public document that is part of CC evaluation	[HCDPP]
External IT Entity	An External Entity that is an IT device (not a human).	[CC] defines "External Entity"

Term	Definition	Source
Field-Replaceable (Unit)	The smallest subassembly that can be swapped in the field to repair a fault.	[IEEE]
Intermediate key	A key used in a point between the initial user authorization and the DEK	[CPP_FDE_E E_V2.0]
Job Owner	A User who initiates or creates a document processing job. It may also refer to a User to whom ownership of a document or job has been delegated or otherwise permitted by the Job Owner.	
Hardcopy Device	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones" and other similar products.	[2600]
Internal Authentication	Identification and authentication function that is wholly contained within the TOE.	
Key Management Description	A non-public document that is part of CC evaluation	[HCDPP]
Local Area Network	A non-public data network in which serial transmission is used without store and forward techniques for direct data communication among data stations located on the User's premises.	[8802-6]
Local User	A User who is physically present at the HCD.	
MFP Administrator	An administrative user with control of one or more aspects of MFP operations.	
MFP Supervisor	An administrative user with control of MFP Administrators	
Modify	Changing the value / content of data in a storage device. Note that in the case of document processing jobs, the outcome is that the instructions or other parameters of the job are changed.	
Multifunction Printer	A device that performs Document printing, scanning, and copying. It may also send and receive Documents over the PSTN using facsimile protocols.	
Network Printing	Printing operation that has been initiated by a Network User.	
Network User	A User who interacts with the HCD over a network.	
Nonvolatile Storage Device	A device that provides computer storage of data that is not cleared when the power is turned off.	
Normal User	A User who is authorized to perform functions that process User Document Data in the TOE.	
Operational Environment	Environment in which the TOE is operated.	[CC]
Organizational Security Policy	Set of security rules, procedures, or guidelines for an organization.	[CC]
Output Tray	A receptacle for the TOE's printed output.	
Protected (TSF) Data	Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.	[2600.1]
Protection Profile	Implementation-independent statement of security needs for a TOE type.	[CC]
Read	To access data from a storage device or data medium. (Note that in this case, the data medium may be a printed output, and therefore, release of a print job is a "read" operation)	[610.12]
Redeploy	The act of moving an HCD from one Operational Environment to another Operational Environment.	



Term	Definition	Source
Security Assurance Requirement	A description of how assurance is to be gained that the TOE meets the SFRs.	[CC]
Security Functional Requirement	A translation of the Security Objectives for the TOE into a standardized language.	[CC]
Security Objective	Statement of an intent to counter identified Threats and/or satisfy identified organization security policies and/or Assumptions.	[CC]
Security Target	Implementation-dependent statement of security needs for a specific identified TOE.	[CC]
Servicing	Performing repairs or preventative maintenance on the HCD.	
Standard Protection Profile	A Protection Profile that is developed according to processes defined by NIAP.	
Submask	A submask is a bit string that can be generated and stored in a number of ways, such as passphrases, tokens, etc.	[CPP_FDE_EE_V2.0]
Target of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance.	[CC]
Temporary Storage	Storage of data that is not intentionally retained by the TOE after the completion of a Document Processing Job.	
Threat	Capabilities, intentions, and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.	[2600.1]
TOE Owner	A person or organizational entity responsible for protecting TOE Assets and establishing related security policies.	[2600.1]
TOE Security Functionality	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.	[CC]
TSF Data	Data for the operation of the TOE upon which the enforcement of the SFR relies.	[CC]
Unauthorized Access	Access to a resource that a User is not permitted to access.	
User	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.	[CC]
User Data	Data for the User that does not affect the operation of the TSF.	[CC]
User Document Data	The Asset that consists of the information contained in a User's Document. This includes the original Document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original Document and printed hardcopy output	[2600.1]
User Job Data	The Asset that consists of the information about a User's Document or job to be processed by the TOE.	[2600.1]

3152 *Table 39 Glossary of Terms*

3153 **Sources:**

3154 [2600] IEEE Std. 2600™-2008 "IEEE Standard for Information Technology: Hardcopy Device and System Security"

3155 [2600.1] IEEE Std. 2600.1™-2009 "IEEE Standard for a Protection Profile in Operational Environment A"

3156 [610.12] IEEE Std 610.12-1990 "IEEE Standard Glossary of Software Engineering Terminology"

3157 [8802-6] ISO /IEC 8802-6:1994 "Information technology – Telecommunications and information exchange  
 3158 between systems – Local and metropolitan area networks – Specific requirements – Part 6"



3159 [CC] ISO/IEC 15408-1:2009 "Information technology – Security techniques – Evaluation criteria for IT security –  
 3160 Part 1"

3161 [CPP\_FDE\_EE\_V2.0] collaborative Protection Profile for Full Drive Encryption – Encryption  
 3162 Engine, Version 2.0, September 09, 2016

3163 [FAR] United States Federal Acquisition Regulations

3164 [HCDPP] "Protection Profile for Hardcopy Devices v1.0"

3165 [IEEE] IEEE Standards Dictionary (ISBN 973-0-7381-2601-2)

3166 **A.2 Acronyms**

Acronym	Definition
BEV	Border Encryption Value
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Service
COTS	Commercial Off-The-Shelf
EAL	Evaluation Assurance Level
HCD	Hardcopy Device
IPA	Information-technology Promotion Agency
I&A	Identification and Authentication
IT	Information Technology
JISEC	Japan Information technology Security Evaluation and Certification scheme
KMD	Key Management Description
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Printer
NIAP	National Information Assurance Partnership
OSP	Organizational Security Policy
PP	Protection Profile
PSTN	Public Switched Telephone Network
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SPP	Standard Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

3167 *Table 40 Acronyms*

3168