RICOH

imagine. change.

## RICOH IM 2500/3000/3500/4000/5000/6000

# Security Target

**Version 1.3**

**August 2021**

**Document prepared by**


www.lightshipsec.com

# Document History

| Version | Date | Description |
|---|---|---|
| 0.1 | 5 Jan 2021 | Initial draft |
| 0.2 | 12 Jan 2021 | Incorporate Ricoh input |
| 0.3 | 3 Feb 2021 | Address lab observations |
| 0.4 | 17 Feb 2021 | Correct FAU_GEN events and update TDs. |
| 0.5 | 9 Mar 2021 | Update user guidance and CAVP references. |
| 0.6 | 12 April 2021 | Addressed CB ORs<br>Updated RSA signature verification references in Table 5<br>Added audit storage clarification. |
| 1.0 | 12 May 2021 | Addressed CB ORs |
| 1.1 | 19 May 2021 | Addressed CB ORs |
| 1.2 | 20 August 2021 | Developer comments and updates after witness testing |
| 1.3 | 31 August 2021 | Addressed CB ORs. |

# Table of Contents

# List of Tables

# 1 Introduction

## 1.1 Overview

1 This Security Target (ST) defines the RICOH IM 2500/3000/3500/4000/5000/6000, version JE-1.00-H Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

## 1.2 Identification

**Table 1: Evaluation identifiers**

| | |
|---|---|
| **Target of Evaluation** | RICOH IM 2500/3000/3500/4000/5000/6000, version JE-1.00-H |
| **Security Target** | RICOH IM 2500/3000/3500/4000/5000/6000 Security Target, v1.3 |

## 1.3 Conformance Claims

2 This ST supports the following conformance claims:

a) CC version 3.1 revision 4

b) CC Part 2 extended

c) CC Part 3 conformant

d) Protection Profile for Hardcopy Devices, v1.0

e) Protection Profile for Hardcopy Devices, v1.0, Errata #1, June 2017

f) NIAP Technical Decisions per Table 2

**Table 2: NIAP Technical Decisions**

| TD # | Name | Rationale if n/a |
|---|---|---|
| TD0074 | FCS_CKM.1(a) Requirement in HCD PP v1.0 | |
| TD0157 | FCS_IPSEC_EXT.1.1 - Testing SPDs | |
| TD0176 | FDP_DSK_EXT.1.2 - SED Testing | |
| TD0219 | NIAP Endorsement of Errata for HCD PP v1.0 | |
| TD0253 | Assurance Activities for Key Transport | |
| TD0261 | Destruction of CSPs in flash | |
| TD0299 | Update to FCS_CKM.4 Assurance Activities | |
| TD0393 | Require FTP_TRP.1(b) only for printing | |
| TD0474 | Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1 | |
| TD0494 | Removal of Mandatory SSH Ciphersuite for HCD | SSH is not claimed. |

| TD # | Name | Rationale if n/a |
|---|---|---|
| TD0562 | Test activity for Public Key Algorithms | SSH is not claimed. |

## 1.4 Terminology

**Table 3: Terminology**

| Term | Definition |
|---|---|
| BEV | Border Encryption Value |
| Firewall | A device to protect the LAN from internet threats. |
| FTP Server | An external IT entity used by the TOE to receive and store user documents |
| HDD | A field-replaceable non-volatile memory storage device, that the TOE uses to store documents, and user accounts information. |
| LAN | Local Area Network — Network used in the TOE environment |
| lc key | A hardware secure module which provides true random number generation and protected storage for the TOE. |
| LDAP Server | An external IT entity used by the TOE for network authentication of users. |
| MFP | Multifunction Printer |
| NVRAM | The NVRAM is a field-replaceable non-volatile storage device where TOE configuration data is stored. |
| PSTN | Public Switched Telephone Network |
| PSTN Line | A connection to a public switched telephone network for the TOE to communicate with external fax machines |
| SMTP Server | An external IT entity used by the TOE for e-mail transmission |
| Syslog Server | An external IT entity used by the TOE for audit log storage |

# 2 TOE Description

## 2.1 Type

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

## 2.2 Usage

4 The expected use cases for the TOE are:

a) **Scanning.** The TOE scans paper documents and then transmits and deletes the scanned images, on command from the Operation Panel.

b) **Printing.** The TOE prints or stores documents received from a printer driver installed on the client computer, and prints or deletes previously stored documents from commands from the Operation Panel or the client computer's web browser.

c) **Copying.** The TOE scans paper documents to be printed.

d) **Network Communications**. The TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). It sends and receives documents over the LAN and the PSTN.

e) **Administration.** The TOE provides management functions to configure and manage its operation. The management functions are accessible locally from the Operation Panel or remotely through the Web Image Monitor (hereafter "WIM") accessible using a web browser on a client computer.

f) **PSTN Faxing.** The TOE provides fax transmission and fax reception functions; both exchange documents according to the Group 3 standard over a Public Switch Telephone Network (PSTN). The Fax Transmission Function sends scanned images of paper documents, or images of electronic documents from a client computer, to external fax devices. The Fax Reception Function receives documents from external fax devices, and stores them in the TOE.

g) **Storage and Retrieval.** The TOE provides a Document Server Function which stores documents and allows users to perform operations on persistently stored documents. From the operation panel, users can store, print and delete documents stored by the document server. From a client computer, users can print and delete documents stored by the document server.

h) **Field-Replaceable Non-volatile Storage.** The TOE stores encrypted data both in the HDD and in NVRAM.

i) **Internal Audit Log Storage.** The MFP stores its audit data internally on the local device in addition to providing the capability for storing them externally to a remote syslog server.

j) **Image Overwrite.** The MFP actively overwrites residual image data stored on the HDD after a document processing job has been completed or cancelled.

### 2.2.1 Deployment

5 As shown in Figure 1, the TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). Other elements of the TOE's operational environment are as shown.

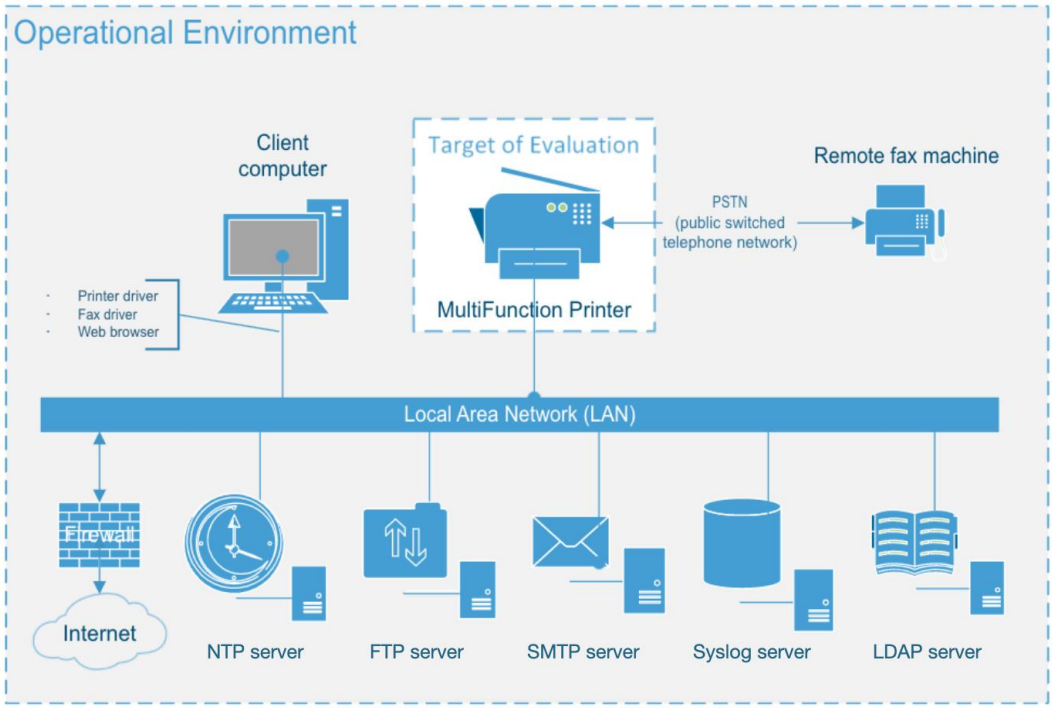



**Figure 1: Example TOE deployment**

### 2.2.2 Interfaces

6 The TOE interfaces include the following:

a) **Operation Panel of the MFP** is an LCD touch screen interface that provides a local user interface where users can perform the following operations:

   i. Configuration of the MFP

   ii. Copying, faxing, storage, and network transmission of paper documents

   iii. Printing, faxing, network transmission, and deletion of the stored documents

   iv. Receiving fax documents via telephone lines and storing them

b) **Web Image Monitor (WIM)** this is the remote user interface accessible via TLS/HTTPS where users can perform the following operations:

   i. Limited configuration of the MFP – various settings

   ii. Operation on stored documents

   iii. Storage and/or printing of documents

   iv. Faxing of documents

c) **Client printer driver or fax driver** is a remote user interface where communication is protected using TLS.

d) **IPsec interface** is used by the TOE to communicate with LDAP, syslog, NTP, SMTP and FTP servers in the TOE operational environment.

e) **TLS interface:** The TOE can be configured to also use TLS to protect communication with a remote syslog or a remote SMTP server.

f) **PSTN Fax Line** is used to connect to a remote fax machine.

## 2.3 Physical Scope

7 The physical boundary of the TOE is comprised of the software and hardware of the MFP models identified in Table 4 (which shows the different RICOH Family Group brand names for the TOE) and related guidance documentation. The TOE is delivered by commercial courier and is installed with the assistance of a RICOH customer engineer.

8 The TOE model number is indicative of copy speed (higher numbers have higher copy speeds) and the alphabetic suffix corresponds to regional fonts and printer languages. The differences between models are not security relevant and are limited to print engine components (speed) and branding variations (labels, displays, packaging materials and documentation).

**Table 4: TOE Models**

| Branding | Model |
|---|---|
| RICOH | RICOH IM 2500, RICOH IM 2500F<br>RICOH IM 3500, RICOH IM 3500F<br>RICOH IM 4000, RICOH IM 4000F<br>RICOH IM 5000, RICOH IM 5000F<br>RICOH IM 6000, RICOH IM 6000F*<br>IM 2500, IM 2500A, IM 2500G<br>IM 3000, IM 3000A, IM 3000G<br>IM 3500, IM 3500A, IM 3500G<br>IM 4000, IM 4000A, IM 4000G<br>IM 5000, IM 5000A, IM 5000G<br>IM 6000, IM 6000G |
| SAVIN | IM 2500, IM 2500A, IM 2500G<br>IM 3000, IM 3000A, IM 3000G<br>IM 3500, IM 3500A, IM 3500G<br>IM 4000, IM 4000G<br>IM 5000, IM 5000G<br>IM 6000, IM 6000G |
| LANIER | |
| nashuatec | IM 2500, IM 2500A<br>IM 3000, IM 3000A |
| Rex Rotary | |

| Branding | Model |
|---|---|
| Gestetner | IM 3500, IM 3500A<br>IM 4000, IM 4000A<br>IM 5000, IM 5000A<br>IM 6000 |

* Models sold in Japan include RICOH in the model name.

9 The TOE includes the following critical components:

a) **Main Controller.** Provides primary printing, scanning, faxing, and networking functionality.

   i) **CPU.** Intel Atom x5-E3930.

   ii) **OS.** LPUX6.0 OS (customized NetBSD 6.0.1).

b) **Operation Unit.** Provides front panel interface control and device extensibility capabilities.

   i) **CPU.** ARM Cortex-A9 Quad Core.

   ii) **OS.** Linux 3.18 (customized).

### 2.3.1 Guidance Documents

10 The TOE guidance documentation includes the following:

a) IM 2500/3000/3500/4000/5000/6000 series User Guide (PDF)

b) User Guide Security Reference (HTML)

c) RICOH IM 2500/3000/3500/4000/5000/6000 Common Criteria Guide, v1.1 (PDF)

## 2.4 Logical Scope

11 The logical scope of the TOE comprises the security functions provided by the TOE to include:

a) **Security Audit.** The TOE generates audit records of user and administrator actions. It stores audit records both locally and on a remote syslog server.

b) **Cryptographic Support.** The TOE includes a cryptographic module for the cryptographic operations that it performs. The relevant CAVP certificate numbers are noted in Table 5 below.

c) **Access Control.** The TOE enforces access control policy to restrict access to user data. The TOE ensures that documents, document processing job information, and security-relevant data are accessible only to authenticated users who have the appropriate access permissions.

d) **Storage Data Encryption.** The TOE encrypts data on the HDD and in NVRAM to protect documents and confidential system information if those devices are removed from the TOE.

e) **Identification and Authentication.** Except for a defined minimal set of actions that can be performed by an unauthenticated user, the TOE ensures that all users must be authenticated before accessing its functions and data. Users login to the TOE by entering their credentials on the local operation

panel, through WIM login, through print or fax drivers, or using network authentication services.

f) **Administrative Roles.** The TOE provides the capability for managing its functions and data. Role-based access controls ensure that the ability to configure the security settings of the TOE is available only to the authorized administrators. Authenticated users can perform copy, printer, scanner, document server and fax operations based on the user role and the assigned permissions.

g) **Trusted Operations.** The TOE performs power-on self-tests to ensure the integrity of the TSF components. It provides a mechanism for performing trusted update that verifies the integrity and authenticity of the upgrade software before applying the updates. It uses an NTP server for accurate time.

h) **TOE Access.** Interactive user sessions at the local and remote user interfaces are automatically terminated by the TOE after a configured period of inactivity.

i) **Trusted Communications.** The TOE protects communications from its remote users using TLS/HTTPS, and communications with the LDAP, FTP, NTP, and SMTP servers using IPsec. The TOE can be configured to use either IPsec or TLS to protect communication with the Syslog and SMTP servers.

j) **PSTN Fax-Network Separation.** The TOE restricts information received from or transmitted to the telephone network to only fax data and fax protocols. It ensures that the fax modem cannot be used to bridge the LAN.

k) **Image Overwrite.** the TOE actively overwrites residual image data stored on the HDD after a document processing job has been completed or cancelled.

### 2.4.1 CAVP Certificates

12 The TOE includes the cryptographic modules with related CAVP certificates shown Table 5 below.

**Table 5: CAVP Certificates**

| Cryptographic Module | Operating Environment | Algorithms | CAVP |
|---|---|---|---|
| RICOH Cryptographic Module for IPSec, v1.0 | Customized NetBSD 6.0.1 on Intel Atom x5-E3930 | AES_CBC | AES 5315 |
| | | SHA2-256<br>SHA2-384<br>SHA2-512 | SHS 4269 |
| | | HMAC-SHA2_256<br>HMAC-SHA2-384<br>HMAC-SHA2-512 | HMAC 3515 |
| RICOH Platform Validation Library for JX3 | BIOS on Intel Atom x5-E3930 | SHA-1 | C630 |

| | | | |
|---|---|---|---|
| RICOH Cryptographic Library 2 (Java), v1.0 | Customized Linux 3.18 on ARM Cortex-A9 Quad Core | SHA-1<br>SHA2-256<br>RSA Signature Verification | C582 |
| libgwguard, v0.9.8a | Customized NetBSD 6.0.1 on Intel Atom x5-E3930 | SHA2-256 | SHS 3231 |
| | | RSA Signature Verification | RSA 2002 |
| RICOH Cryptographic Library C, v1.2 | Customized Linux 3.18 on ARM Cortex-A9 Quad Core | ECDSA signature verification<br>Curve P-256<br>SHA2-256 | C629 |
| LPUX NVRAM Encryption Driver, v1.2 | Customized NetBSD 6.0.1 on Intel Atom X5-E3930 | AES-CBC<br>Encryption/decryption<br>Key length: 256 | AES 4560 |
| Boot SHA-1 Module, v47.04 | ST33TPHF2ESPI | SHA-1 | C715 |
| RICOH Company<br>AES256CBC Implementation | MB8AL1062MH-GE1 | AES-CBC<br>Encrypt, Decrypt<br>Key Length: 256 | AES 3921 |
| wolfCrypt, v4.1.1 | NetBSD v6.0.1 on Intel Atom Apollo Lake E3930 (Goldmont) | RSA Key Generation<br>RSA Signature Generation (PKCS 1.5)<br>RSA Signature Verification (PKCS 1.5) | A1837 |
| | | ECDHE | |
| | | ECDSA | |
| | | SHA-1, SHA2-256, SHA2-384, SHA2-512 | |
| | | AES-CBC<br>AES-GCM<br>Encryption/decryption<br>Key length 128, 256 | |
| | | HMAC-SHA-1 | |

| | | | |
|---|---|---|---|
| | | HMAC-SHA2-256<br>HMAC-SHA2-384<br>HMAC-SHA2-512 | |
| | | DRBG | |

### 2.4.2 Excluded Features

13 The following features of the MFP are excluded from the evaluated configuration:

a) **USB Port.** The MFP has a USB Port that is used to directly connect a client computer to the MFP for printing. This USB port is disabled during initial installation and configuration of the TOE.

b) **SD Card Slot.** The MFP has two SD Card Slots, one for customer engineers and one for users. The SD Card Slot for customer engineer is used by customer engineers to install components of the MFP; the SD Card Slot for users is used by users to print documents. Both are disabled when the TOE is operational, a cover is placed on the SD Card slot for customer engineer so cards cannot be inserted or removed and the card slot for users is set to disabled during installation.

### 2.4.3 Required non-TOE Components

14 The following non-TOE components are required in the TOE operational environment:

a) **Syslog Server.** The TOE uses a remote syslog server for long term storage of its audit trail.

b) **LDAP Server.** The TOE uses an LDAP server for user authentication.

c) **NTP Server.** The TOE ensures accurate time by synchronizing with a remote NTP server.

d) **FTP Server.** The TOE stores user documents on a remote FTP server.

e) **SMTP Server.** The TOE uses an SMTP server for email transmission.

# 3 Security Problem Definition

15 The Security Problem Definition is reproduced from section 2 of the HCDPP.

## 3.1 Users

16 There are two categories of Users defined in this ST, Normal and Admin.

**Table 6: User Categories**

| Designation | Name | Definition |
|---|---|---|
| U.NORMAL | Normal User | A User who has been identified and authenticated and does not have an administrative role |
| U.ADMIN | Administrator | A User who has been identified and authenticated and has an administrative role |

17 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

18 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:

**Table 7: Asset Categories**

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

19 There are no additional Asset categories defined in this ST.

### 3.2.1 User Data

20 User Data are composed of two types:

**Table 8: User Data Types**

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

21 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:

**Table 9: Document and Job Attributes**

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

### 3.2.2 TSF Data

22 TSF Data are composed of two types:

**Table 10: TSF Data 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 |

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

#### 3.2.2.1 Protected TSF Data

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

a) Username
b) Number of Attempts before Lockout
c) Settings for Lockout Release Timer
d) Lockout time
e) Date settings (year/month/day)
f) Time settings
g) Minimum Character No.
h) Password Complexity Setting

i) Operation Panel auto logout time

j) WIM auto logout time

k) Stored Reception File User

l) Document user list

m) Available function list

n) User authentication method

o) Device Certificate

p) Network settings

q) Audit transfer settings

r) TOE Software

#### 3.2.2.2 Confidential TSF Data

25 D.TSF.CONF is composed of the following data:

a) Login password

b) Audit log

c) HDD cryptographic key

## 3.3 Threats

26 The following threats are mitigated by this TOE:

**Table 11: Threats**

| Identifier | Description |
|---|---|
| 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_UP DATE | 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. |

## 3.4 Assumptions

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

**Table 12: Assumptions**

| Identifier | Description |
|---|---|
| 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. |

## 3.5 Organizational Security Policies

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

**Table 13: Organizational Security Policies**

| Identifier | Description |
|---|---|
| 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 | If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Non-volatile Storage Devices, it will encrypt such data on those devices. |
| P.KEY_MATERIAL | 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 | If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN. |
| P.IMAGE_OVERWRITE | Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices. |

# 4 Security Objectives

29 The following Security Objectives are satisfied by this TOE:

**Table 14: Security Objectives for the TOE**

| Identifier | Description |
|---|---|
| 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 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.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 | 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 | 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 | 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 | Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices. |

30 The following Security Objectives must be satisfied by the TOE's Operational Environment.

**Table 15: Security Objectives for the Operational Environment**

| Identifier | Description |
|---|---|
| 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. |

# 5 Security Requirements

## 5.1 Conventions

31 This document uses the following font conventions to identify the operations defined by the CC:

c) **Assignment.** Indicated with italicized text.

d) **Refinement.** Indicated with bold text and strikethroughs.

e) **Selection.** Indicated with underlined text.

f) **Assignment within a Selection:** Indicated with italicized and underlined text.

g) **Iteration.** Indicated by adding letter in parentheses for iterations completed in the PP. Iterations completed in the ST are identified by adding a string starting "/" (e.g. "FCS_CKM.1(b)/DIM"

**Note:** operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the HCDPP.

## 5.2 Extended Components Definition

32 Refer to Annex A: Extended Components Definition.

## 5.3 Functional Requirements

**Table 16: Summary of SFRs**

| Requirement | Title |
|---|---|
| FAU_GEN.1 | Audit Data Generation |
| FAU_GEN.2 | User Identity Association |
| FAU_SAR.1 | Audit Review |
| FAU_SAR.2 | Restricted Audit Review |
| FAU_STG.1 | Protected Audit Trail Storage |
| FAU_STG_EXT.1 | Protected Audit Event Storage |
| FAU_STG.4 | Prevention of Audit Data Loss |
| FCS_CKM.1(a) | Cryptographic Key Generation (for asymmetric keys) |
| FCS_CKM.1(b)/DAR | Cryptographic Key Generation (for Symmetric keys) [Data At Rest] |
| FCS_CKM.1(b)/DIM | Cryptographic Key Generation (for Symmetric keys) [Data In Motion] |
| FCS_CKM_EXT.4 | Extended: Cryptographic Key Material Destruction |

| Requirement | Title |
|---|---|
| FCS_CKM.4 | Cryptographic Key Destruction |
| FCS_COP.1(a) | Cryptographic Operation (Symmetric Encryption/Decryption) |
| FCS_COP.1(b) | Cryptographic Operation (Signature Generation and Verification) |
| FCS_COP.1(c)/L1 | Cryptographic Operation (Hash Algorithm) |
| FCS_COP.1(c)/L2 | Cryptographic Operation (Hash Algorithm) |
| FCS_COP.1(d) | Cryptographic Operation (AES Data Encryption/Decryption) |
| FCS_COP.1(f) | Cryptographic Operation (Key Encryption) |
| FCS_COP.1(g) | Cryptographic Operation (for keyed-hash message authentication) |
| FCS_HTTPS_EXT.1 | Extended: HTTPS selected |
| FCS_IPSEC_EXT.1 | Extended: IPsec selected |
| FCS_KYC_EXT.1 | Extended: Key Chaining |
| FCS_RBG EXT.1 | Extended: Cryptographic Operation (Random Bit Generation) |
| FCS_TLS_EXT.1 | Extended: TLS selected |
| FDP_ACC.1 | Subset Access Control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_DSK_EXT.1 | Extended: Protection of Data on Disk |
| FDP_FXS_EXT.1 | Extended: Fax separation |
| FDP_RIP.1(a) | Subset residual information protection |
| FIA_AFL.1 | Authentication Failure Management |
| FIA_ATD.1 | User attribute definition |
| FIA_PMG_EXT.1 | Extended Password Management |
| FIA_PSK_EXT.1 | Extended: Pre-Shared Key Composition |
| FIA_UAU.1 | Timing of authentication |
| FIA_UAU.7 | Protected Authentication Feedback |
| FIA_UID.1 | Timing of identification |

| Requirement | Title |
|---|---|
| FIA_USB.1 | User-subject binding |
| FMT_MOF.1 | Management of security functions behavior |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.3 | Static attribute initialization |
| FMT_MTD.1 | Management of TSF Data |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Restrictions on Security Roles |
| FPT_KYP_EXT.1 | Extended: Protection of Key and Key Material |
| FPT_SKP_EXT.1 | Extended: Protection of TSF Data |
| FPT_STM.1 | Reliable Time Stamps |
| FPT_TST_EXT.1 | Extended: TSF testing |
| FPT_TUD_EXT.1 | Extended: Trusted update |
| FTA_SSL.3 | TSF-initiated Termination |
| FTP_ITC.1/TLS | Inter-TSF trusted channel |
| FTP_ITC.1/IPsec | Inter-TSF trusted channel |
| FTP_TRP.1(a) | Trusted Path (for Administrators) |
| FTP_TRP.1(b) | Trusted Path (for Non-administrators) |

### 5.3.1 Security Audit (FAU)

**FAU_GEN.1 Audit Data Generation**

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;

c) All auditable events specified in Table 17: Audit Events, [*no other 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 17**, [*no other audit relevant information*].

**Table 17: Audit Events**

| 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 |
| Failure to establish session | FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b) | Reason for failure |

### FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### FAU_SAR.1 Audit Review

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

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

### FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

### FAU_STG.1 Protected Audit Trail Storage

FAU_STG1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

### FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

### FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 Refinement The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

## 5.3.2 Cryptographic Support (FCS)

### FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1(a) Refinement The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [**

- NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for finite field-based key establishment schemes;
- NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for elliptic curve-based key establishment schemes and implementing “NIST curves” P256, P-384 and [P-521] (as defined in FIPS PUB 186-4, “Digital Signature Standard”)

**]**

**and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**

### FCS_CKM.1(b)/DAR Cryptographic Key Generation (Symmetric keys)/Data At Rest

FCS_CKM.1.1(b)/DAR Refinement The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [256 bit] that meet the following: No Standard.**

### FCS_CKM.1(b)/DIM Cryptographic Key Generation (Symmetric keys)/Data In Motion

FCS_CKM.1.1(b)/DIM Refinement The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [128 bit, 256 bit] that meet the following: No Standard.**

### FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.4.1 Refinement The TSF shall destroy **all plaintext secret and private cryptographic keys and cryptographic critical security parameters** when no longer needed.

### FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 Refinement The TSF shall destro**y** cryptographic keys in accordance with a specified cryptographic key destruction method [

- For volatile memory, the destruction shall be executed by [selection: removal of power to the memory];
- For nonvolatile storage, the destruction shall be executed by a [ [single] overwrite consisting of [a new value of a key of the same size]];

] that meets the following: No Standard.

Application Note: This SFR is altered by TD0261.

### FCS_COP.1(a) Cryptographic Operation (Symmetric Encryption/Decryption)

FCS_COP.1.1(a) Refinement The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [*CBC mode, GCM mode*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[NIST SP 800-38A, NIST SP 800-38D]**

### FCS_COP.1(b) Cryptographic Operation (for Signature Generation/ Verification)

FCS_COP.1.1(b) Refinement The TSF shall perform **cryptographic signature services** in accordance with a **[**

- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [*2048 bits*]**]**
- Elliptic Curve Digital Signature Algorithm (ECDSA) with key size of [256 bits or greater]]

that meets the following: [

Case: RSA Digital Signature Algorithm:

- FIPS PUB 186-4, "Digital Signature Standard"

Case: ECDSA Digital Signature Algorithm:

- FIPS PUB 186-4, "Digital Signature Standard"
- The TSF shall implement "NIST curves" P-256, P384 and [P521] (as defined in FIPS PUB 186-4, "Digital Signature Standard").]

### FCS_COP.1(c)/L1 Cryptographic Operation (Hash Algorithm)

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

### FCS_COP.1(c)/L2 Cryptographic Operation (Hash Algorithm)

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

### FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)

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

### FCS_COP.1(f) Cryptographic Operation (Key Encryption)

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

### FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

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

### FCS_HTTPS_EXT.1 Extended: HTTPS selected

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement the HTTPS protocol using TLS as specified in FCS_TLS_EXT.1.

### FCS_IPSEC_EXT.1 Extended: IPsec selected

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [transport mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC].

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

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1] protocol uses the cryptographic algorithms [no other algorithm].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

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

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [[No *other DH groups*]].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [RSA] algorithm and Pre-shared Keys.

Application Note: This SFR is altered by TD0157

### FCS_KYC_EXT.1 Extended: Key Chaining

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

### FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [NIST SP 800-90A] using [Hash_DRBG (**~~any~~ SHA-256**)].

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

### FCS_TLS_EXT.1 Extended: TLS selected

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following cipher suites:

[

- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384]

Application Note: This SFR is altered by TD0474

## 5.3.3 User Data Protection (FDP)

### FDP_ACC.1 Subset access control

FDP_ACC.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in ~~**Table 2 and Table3**~~ Table 18 **and** Table 19**.**

### FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in ~~**Table 2 and Table3**~~ Table 18 **and** Table 19**.**

FDP_ACF.1.2 Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in ~~Table 2 and Table3~~** Table 18 **and** Table 19**.**

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

**Table 18: D.USER.DOC Access Control SFP**

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| **Print (+PRT)** | Operation: | Submit a document to be printed | View image or Release printed output | Modify stored document | Delete stored document |

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| | Job owner | Allowed (note 1) | View: Allowed Release: allowed | No function | Allowed |
| | U.ADMIN | No function | View: no function Release: no function | No function | Allowed |
| | U.NORMAL | Allowed | Denied | Denied | Denied |
| | Unauthenticated | (condition 1) | Denied | Denied | Denied |
| **Scan (+SCN)** | Operation: | Submit a document for scanning | View scanned image | Modify stored image | Delete stored image |
| | Job owner | Allowed (note 2) | Allowed | No function | Allowed |
| | U.ADMIN | No function | No function | No function | Allowed |
| | U.NORMAL | Allowed | Denied | Denied (No function) | Denied (No function) |
| | Unauthenticated | Denied | Denied | Denied (No function) | Denied (No function) |
| **Copy (+CPY)** | Operation: | Submit a document for copying | View scanned image or Release printed copy output | Modify stored image | Delete stored image |
| | Job owner | Allowed (note 2) | View: no function Release: no function | No function | No function |
| | U.ADMIN | No function | View: no function Release: no function | No function | No function |
| | U.NORMAL | Allowed | Denied | Denied (No function) | Denied (No function) |

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

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| | U.NORMAL | Allowed | Denied | Denied | Denied |
| | Unauthenticated | (condition 1) | Denied | Denied | Denied |

**Table 19: D.USER.JOB Access Control SFP**

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| **Print (+PRT)** | Operation: | Create print job | View print queue / log | Modify print job | Cancel print job |
| | Job owner | (note 1) | Allowed | No function | Allowed |
| | U.ADMIN | No function | Allowed | No function | Allowed |
| | U.NORMAL | Allowed | Allowed | Denied | Denied |
| | Unauthenticated | Denied | Allowed | Denied | Denied |
| **Scan (+SCN)** | Operation: | Create scan job | View scan status / log | Modify scan job | Cancel scan job |
| | 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)** | Operation: | Create copy job | View copy status / log | Modify copy job | Cancel copy job |
| | Job owner | (note 2) | Allowed | No function | Allowed |
| | U.ADMIN | No function | Allowed | No function | Denied |
| | U.NORMAL | Allowed | Allowed | Denied | Denied |
| | Unauthenticated | Denied | Denied | Denied | Denied |
| **Fax send (+FAXOUT)** | Operation: | Create fax send job | View fax job queue / log | Modify fax send job | Cancel fax send job |
| | Job owner | (note 2) | Allowed | Allowed | no function |
| | U.ADMIN | No function | Allowed | No function | no function |

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| | U.NORMAL | Allowed | Allowed | Denied | Denied |
| | Unauthenticated | Denied | Denied | Denied | Denied |
| **Fax receive (+FAXIN)** | Operation: | Create fax receive job | View fax receive status / log | Modify fax receive job | Cancel fax receive job |
| | 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)** | Operation: | Create storage / retrieval job | View storage / retrieval log | Modify storage / retrieval job | Cancel storage / retrieval job |
| | 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 |

Application notes:

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

See also the following Notes that are referenced in ~~**Table 2 and Table3**~~ Table 18 **and** Table 19**.**

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

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

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

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

Note 5: Viewing is not permitted and releasing the document is permitted.

Note 6: Secure Fax must be enabled.

### FDP_DSK_EXT.1 Extended: Protection of Data on Disk

FDP_DSK_EXT.1.1 The TSF shall [perform encryption in accordance with FCS_COP.1(d)] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

**FDP_FXS_EXT.1 Extended: Fax separation**

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

**FDP_RIP.1(a) Subset residual information protection**

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: **D.USER.DOC.**

### 5.3.4 Identification and Authentication (FIA)

**FIA_AFL.1 Authentication Failure Management**

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*1 to 10*]] unsuccessful authentication attempts occur related to [

- 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].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [lock the user account for an administrator configurable time period, or until an administrator unlocks the account.].

Application Note: This SFR applies only to internal identification and authentication.

**FIA_ATD.1 User attribute definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Username, User Role, Available Functions List*]

**FIA_PMG_EXT.1 Extended: Password Management**

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [ “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [[“””, “”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[”, “\”, “]”, “_”, “`”, “{”, “|”, “}”, “~”]];

b) Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

### FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

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

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [SHA-256] and be able to [use no other pre-shared keys].

### FIA_UAU.1 Timing of authentication

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

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

### FIA_UAU.7 Protected Authentication Feedback

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

### FIA_UID.1 Timing of identification

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

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*username, available function list, and user role*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*an*

*Available functions list is associated with the user after the user is authenticated*, *and the set of available functions does not change during the user session*.]

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

### 5.3.5 Security Management (FMT)

#### FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 Refinement The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [listed in Table 20] to **U.ADMIN**.

#### FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 Refinement The TSF shall enforce **the User Data Access Control SFP** to restrict the ability to [query, modify] the security attributes [*username available function list, user role]*to [*U.ADMIN*].

#### FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 Refinement The TSF shall allow the **[U.ADMIN]** to specify alternative initial values to override the default values when an object or information is created.

#### FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 Refinement The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in ~~Table~~ 4** Table 20

**Table 20: Management of TSF Data**

| Data | Operation | Interfaces | Authorized Role(s) |
|---|---|---|---|
| *TSF Data owned by U.NORMAL or associated with documents or jobs owned by U.NORMAL.* | | | |
| *Login password for authenticated user* | Modify | Operation Panel, WIM | The Owning U.NORMAL or U.ADMIN |
| | *TSF Data not owned by a U.NORMAL* | | |
| *Audit Logs* | Delete, export | WIM | U.ADMIN |

| Data | Operation | Interfaces | Authorized Role(s) |
|---|---|---|---|
| *Login passwords of U.ADMIN user* | Modify | Operation Panel, WIM | U.ADMIN |
| *Username, user role, available function list or access permissions of U.NORMAL Users* | Modify | Operation Panel, WIM | U.ADMIN |
| *HDD Cryptographic Key* | Create, Delete | Operation Panel | U.ADMIN |
| *Software, firmware, and related configuration data* | | | |
| *Audit Transfer Settings* | Modify | Operation Panel, WIM | U.ADMIN |
| *Date & Time Settings* | Modify | WIM | U.ADMIN |
| *Password Length and Password complexity settings* | Modify | Operation Panel, WIM | U.ADMIN |
| *Operation Panel Auto logout settings* | Modify | Operation Panel, WIM | U.ADMIN |
| *WIM Auto logout settings* | Modify | WIM | U.ADMIN |
| *PSTN Fax-Line Separation - Stored Reception File User* | Modify | Operation Panel | U.ADMIN |
| *Device Certificate* | Create, Query, Modify, Delete | Operation Panel, WIM | U.ADMIN |
| *TOE Software updates* | Modify | WIM | U.ADMIN |
| *Network settings for trusted communication* | Modify | Operation Panel, WIM | U.ADMIN |

### FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 Refinement The TSF shall be capable of performing the following management functions: [*management functions listed in* Table 21.

**Table 21: Management Functions**

| Management Functions | Operation | Interface(s) |
|---|---|---|
| Manage user accounts (users, roles, privileges and available functions list) | Create, modify, delete | Operation Panel, WIM |
| Manage the document user list for stored documents | Create, modify | Operation Panel, WIM |
| Configure audit transfer settings | Modify | WIM |
| Manage audit logs | Delete, export | Operation Panel, WIM |
| Manage Audit Functions | Enable, Disable | Operation Panel, WIM |
| Manage time and date settings | Modify | Operation Panel, WIM |
| Configure minimum password length | Modify | Operation Panel, WIM |
| Configure Password complexity settings | Modify | Operation Panel, WIM |
| Configure Operation Panel Auto Logout Time | Modify | Operation Panel, WIM |
| Configure WIM Auto Logout Time | Modify | WIM |
| Configure number of authentication failure before account lockout | Modify | WIM |
| Configure account release timer settings | Modify | WIM |
| Configure PSTN Fax-Line Separation Stored Reception File User | Modify | Operation Panel, WIM |
| Configure image overwrite | Modify | Operation Panel, WIM |
| Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE) | Modify | Operation Panel, WIM |
| Manage HDD Cryptographic key | Create Delete | Operation Panel |
| Manage Device Certificates | Create, query, modify, delete, upload, download | Operation Panel, WIM |

| Management Functions | Operation | Interface(s) |
|---|---|---|
| Manage TOE Trusted Update | Query, Modify | WIM |
| Configure IPSec | Modify | WIM |
| Configure SMTP over IPSec | Modify | WIM |
| Configure NTP | Modify | WIM |
| Manage user accounts (Ability to login) | Unlock | WIM |

**FMT_SMR.1 Restrictions on Security Roles**

FMT_SMR.1.1 Refinement The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

### 5.3.6 Protection of the TSF (FPT)

**FPT_KYP_EXT.1 Extended: Protection of Key and Key Material**

FPT_ KYP _EXT.1.1 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.**

**FPT_SKP_EXT.1 Extended: Protection of TSF Data**

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

**FPT_STM.1 Reliable Time Stamps**

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

**FPT_TST_EXT.1 Extended: TSF testing**

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

**FPT_TUD_EXT.1 Extended: Trusted update**

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [no other functions] prior to installing those updates.

### 5.3.7 TOE Access (FTA)

#### FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate 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*].

### 5.3.8 Trusted path/channels (FTP)

#### FTP_ITC.1/TLS Inter-TSF trusted channel

FTP_ITC.1.1/TLS Refinement The TSF shall use **[TLS] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [[*syslog, SMTP*]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**

FTP_ITC.1.2/TLS Refinement The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel.

FTP_ITC.1.3/TLS Refinement The TSF shall initiate communication via the trusted channel for [***communication via the LAN of document data, function data, protected data, and confidential data***].

#### FTP_ITC.1/IPsec Inter-TSF trusted channel

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

FTP_ITC.1.2/IPsec Refinement The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel.

FTP_ITC.1.3/IPsec Refinement The TSF shall initiate communication via the trusted channel for [*communication via the LAN of document data, function data, protected data, and confidential data*].

#### FTP_TRP.1(a) Trusted Path (for Administrators)

FTP_TRP.1.1(a) Refinement The TSF shall **use [TLS/HTTPS] to** provide **a trusted** communication path between itself and remote administrators that is

logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data.**

FTP_TRP.1.2(a) Refinement The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3(a) Refinement The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions.**

### FTP_TRP.1(b) Trusted Path (for Non-administrators)

FTP_TRP.1.1(b) Refinement The TSF shall **use [TLS/HTTPS] to** provide **a trusted** communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data.**

FTP_TRP.1.2(b) Refinement The TSF shall permit [the TSF, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3(b) Refinement The TSF shall require the use of the trusted path for **initial user authentication and all remote actions.**

## 5.4 Assurance Requirements

33 The TOE security assurance requirements are summarized in Table 22. See Annex B for Security Assurance Requirements description.

**Table 22: TOE Security Assurance Requirements**

| Assurance Class | Components | Description |
|---|---|---|
| Security Target Evaluation | ASE_CCL.1 | Conformance Claims |
| | ASE_ECD.1 | Extended Components Definition |
| | ASE_INT.1 | ST Introduction |
| | ASE_OBJ.1 | Security Objectives for the operational environment |
| | ASE_REQ.1 | Stated Security Requirements |
| | ASE_SPD.1 | Security Problem Definition |
| | ASE_TSS.1 | TOE Summary Specification |
| 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 |

# 6 TOE Summary Specification

34 The following describes how the TOE fulfils each SFR included in section 5.3.

## 6.1 Security Audit

### 6.1.1 FAU_GEN.1 & FAU_GEN.2

35 The TOE records an audit log of events listed in Table 23. Audit log entries record the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Additionally, Job Completion events record the type of job, and Failure to Establish Session events record the reason for such failure.

**Table 23: List of Audit Events**

| 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 |

| Auditable event requirements | Auditable events satisfied |
|---|---|
| | 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 |

### 6.1.2 FAU_STG.1, FAU_STG_EXT.1, FAU_STG.4, FAU_SAR.1, FAU_SAR.2, FTP_ITC.1/IPsec and FTP_ITC.1/TLS

36 The TOE stores audit log data in a dedicated storage area of the HDD. Audit records are buffered in that storage area before transfer to a configured remote syslog server over a configured TLS or an IPsec trusted channel.

37 Authorized administrators use the WIM to review the audit trail and to initiate transfer of audit records. The TOE prevents unauthorized access to the audit records by ensuring that the options to manage the audit function and the audit records are not included in the lists of available functions visible to the U.NORMAL users.

38 The TOE audit trail comprises three types of audit logs: Job logs, Access logs, and Ecology logs. By default, the job and ecology logs will each hold a maximum of 4,000 records; the access log can have a maximum of 12,000 records. When a maximum number of records is reached, the records are overwritten based on the following criteria:

a) When syslog audit transfers are working, the oldest records which have been transferred to the syslog server are overwritten first.

b) If none of the logs have been transferred to the audit server, the oldest records are overwritten first.

## 6.2 Identification and Authentication

### 6.2.1 FIA_UAU.1, FIA_UID.1, FIA_UAU.7, FIA_ATD.1 & FIA_USB.1

39 For each individual user, the TOE maintains the user attributes: username, password, user role and available functions list regardless of the authentication method for the user account. Users login to the TOE by entering their username/password credentials on the Operation Panel, the WIM login screen, or through a client's print driver or fax driver that has been configured to submit user credentials.

40 When users enter their passwords on the Operation Panel or the WIM login, the TOE displays a sequence of dummy characters whose length is the same as that of the entered password.

41 All users accessing the TOE user interfaces are identified and authenticated before they are allowed access. Only the following functions are accessible before the user is authenticated:

a) Viewing user job lists, WIM Help, system status, the counter and information of inquiries.

b) Creation of fax reception jobs.

c) Creation of print jobs

42 The TOE authenticates users by checking the entered username/passwords credentials against the local user database or against an external authentication service (LDAP).

43 An available functions list that identifies the basic hardcopy functions a user is permitted to perform is associated with each Normal User. After successful login, users are authorized to perform functions according to their assigned user role (Normal User, MFP Administrator, or MFP Supervisor). If login fails, the user is not denied access to all functions that require user authentication.

### 6.2.2 FIA_PMG_EXT.1

44 For authentication within the TOE, login passwords for users can be registered only if these passwords meet the conditions specified by the selections in FIA_PMG_EXT.1.

### 6.2.3 FIA_AFL.1 & FTA_SSL.3

45 The TOE counts consecutive login failures for a given login name and will locks out that user after an administrator-configured number of authentication failures attempts have been reached. For the U.NORMAL users, the account lockout is released when the configured lockout time has elapsed or by direct release operation performed by the MFP administrator. For the U.ADMIN users, the account lockout is released when the configured lockout time has elapsed, or by direct release operation performed by the MFP Administrator or MFP Supervisor, or by elapse of a given time after the TOE restarts.

46 The TOE can terminate user sessions at the various interfaces as follow:

h) **Operation Panel**: the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time (settable from 10 to 999 seconds).

i) **WIM**: the user is logged out of the TOE when inactivity reaches the WIM auto logout time (settable from 3 to 60 minutes).

j) **Printer driver**: the user is logged out of the TOE immediately after receiving the print data from the printer driver.

k) **Fax driver**: the user is logged out of the TOE immediately after receiving the transmission information from the fax driver.

## 6.3 Access Control

### 6.3.1 FDP_ACC.1 & FDP_ACF.1

47 The TOE controls user operations for document data and user jobs as specified in Table 18 and Table 19.

#### 6.3.1.1 Access control rule on document data

48 The TOE provides users with the ability to perform operations on document data that are stored in the TOE.

49 Normal Users are permitted to operate on document data if the ID of the user corresponds to the Document User List for that document (i.e., the user is the "Job Owner"). A Normal User is not permitted to operate on document data for which it is not the Job Owner.

50 A Normal User who is a Job Owner may print, download to client computers, send by fax, send by e-mail as attachments, and delete stored documents, using the Operation Panel or a web browser.

51 The TOE allows only the Job Owner to view and delete the document data handled as a user job while Copy Function, Printer Function, Scanner Function, Fax Function, or Document Server Function is being used.

52 While no interface to change job owners is provided, an interface to cancel user jobs is provided. If a user job is cancelled, any document the cancelled job operates will be deleted.

**Table 24: Stored Documents Access Control Rules for Normal Users**

| Function | User interface | Type of document | Operations permitted for authorized users |
|---|---|---|---|
| Printer | Operation Panel | +PRT | Print<br>Delete |
| Printer | Web browser | +PRT | Delete |
| Scanner | Operation Panel | +SCN | E-mail transmission |
| Fax | Operation Panel | +FAXIN | Print<br>Delete |
| Fax | Web browser | +FAXIN | Download<br>Delete<br>(Operations above are permitted only if Normal Users are authorized to use Document Server Function) |
| Document Server | Operation Panel | +DSR | Print<br>Delete |
| Document Server | Operation Panel | +FAXOUT | Print<br>Delete |
| Document Server | Web browser | +DSR | Delete |
| Document Server | Web browser | +FAXOUT | Fax transmission<br>Download |

| Function | User interface | Type of document | Operations permitted for authorized users |
|---|---|---|---|
| | | | Delete<br>(Fax transmission is permitted for Normal Users who are authorized to use Fax Function) |

53 MFP Administrators are not permitted to print, download, or send stored documents. MFP Administrators may delete stored documents, using the Operation Panel, web browser, or indirectly by cancelling a job.

54 The MFP Supervisor is not permitted to perform any document operations.

#### 6.3.1.2 Access control rule on user jobs

55 The TOE displays on the Operation Panel a menu to cancel a user job only if the user who logs in from the Operation Panel is a Job Owner or MFP Administrator and a cancellation of a user job is attempted by the Job Owner or an MFP Administrator. Other users are not allowed to operate user jobs.

56 When a user job is cancelled, any documents operated by the cancelled job will be deleted. However, if the document data operated by the cancelled user job is a stored document, the data will not be deleted and remain stored in the TOE.

## 6.4 Cryptographic Operations

### 6.4.1 FCS_CKM.1 (a), FCS_CKM.1(b)/DIM, FCS_CKM.1(b)/DAR, FCS_RBG_EXT.1.

57 The TOE implements random-bit generation services using a software based-based DRGB that has been seeded with at least 256-bits of entropy from a third-party hardware-based TRNG and DRBG.

**Table 25: Random Number Sources**

| RNG | Method | Standard | RNG |
|---|---|---|---|
| **Hardware TRNG** | True RNG + DRBG | AIS31 Class 2 | Hardware TRNG |
| **Software DRBG** | Hash_DRBG_SHA256 | SP 800-90A | Software DRBG |

58 The TOE generates cryptographic keys upon initial start-up, as a result of administrative actions and during communication sessions. Using a Hash-DRBG, the TOE generates a KEK, HDD Key, NVRAM Key and DevCert Key, which it uses for data encryption; TLS session keys, IPsec IKE key and ESP key which it uses for trusted communications.

For all encryption operations the TOE uses AES 256 in CBC mode and the following cryptographic keys:

a) FFC DH Groups 14 (2048-bit MODP)

b) ECDHE P-256, P-384, P-521

c) RSA 2048

d) 128-bit and 256-bit symmetric keys

59 Additional details about key creation, the TRNG, and the DRBG, are provided in the Key Management Description and Entropy Description documents.

### 6.4.2 FPT_SKP_EXT.1, FCS_CKM.4 and FCS_CKM_EXT.4

60 All pre-shared keys, symmetric keys, and private keys are protected in storage and are not accessible to any user through TOE interfaces. A root encryption key is securely stored in IcKey (a Trusted Platform Module). No other plaintext keys are stored in non-volatile storage. The root encryption key is used to decrypt a key encryption key which is used to decrypt symmetric keys for encrypted storage and the Device Certificate. The IPsec PSK is stored in an encrypted partition of NVRAM. Key destruction is described in the Key Management Description.

61 The TOE destroys cryptographic keys and key materials when no longer needed. TLS and IPsec session keys are no longer needed at the end of a communication session. The REK, KEK, NVRAM Key, and DevCert Key are always needed and are never destroyed in the evaluated configuration. HDD encryption is always enabled in the evaluated configuration, so the HDD key is always needed. Cryptographic keys and key materials stored by the TOE can be destroyed by overwriting the key with the value of a new key; the HDD key can be logically deleted should HDD encryption be disabled. Key destruction is further described in the separate proprietary Key Management Document (KMD).

## 6.5 Stored Data Encryption

### 6.5.1 FCS_KYC_EXT.1, FPT_KYP_EXT.1, and FCS_COP.1(f)

62 The TOE encrypts data on the HDD and in NVRAM. The keychain for encrypting field-replaceable non-volatile storage devices begins with a common Root Encryption Key (REK). The plaintext REK is stored in a hardware security module, Ic Key.

63 The REK is used to encrypt and decrypt a Key Encryption Key (KEK). The KEK is used to encrypt and decrypt Device Encryption Keys (DEKs) for the HDD and NVRAM. All such operations use 256-bit AES keys to protect 256-bit AES data encryption on the target devices.

**Table 26: Keychain encryption**

| Key | En/decrypts | Algorithm | Length | SFR |
|---|---|---|---|---|
| **Root Encryption Key (REK)** | Key Encryption Key | AES CBC | 256 | FCS_COP.1(f) |
| **Key Encryption Key (KEK)** | HDD Key<br>NVRAM Key<br>DevCert Key | AES CBC | 256 | FCS_COP.1(f) |

64 Additional details about the keychain and device encryption are provided in the Key Management Description.

### 6.5.2 FDP_DSK_EXT.1 and FCS_COP.1(d)

65 Two field-replaceable non-volatile storage devices employ encryption: the HDD, and NVRAM.

66 All HDD data is encrypted with AES 256 CBC encryption by a hardware component, Ic Ctrl. HDD encryption is enabled and initialized in the evaluated configuration, as described in the guidance documentation.

67 Partition 3 of NVRAM is encrypted software component, LPUX NVRAM Encryption Driver, with AES 256 CBC encryption. NVRAM encryption is initialized during manufacturing and cannot be disabled. Other partitions of NVRAM do not contain confidential User or TSF Data.

68 Keychain, key management, and other details are provided in the Key Management Description.

## 6.6 Protection of the TSF

### 6.6.1 FPT_STM.1

69 The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from the system clock of the TOE. The system clock is also used for other time-related functions, including user lockout timing, idle session timeouts, and SA lifetimes.

70 The system clock may be set locally or configured to use a network time server. Only an MFP Administrator can configure the system clock.

## 6.7 Trusted Communications

71 The Trusted Communications Function provides trusted paths for communications between the TOE and remote users / external IT entities.

### 6.7.1 FTP_TRP.1 (a), FTP_TRP.1 (b), FCS_HTTPS_EXT.1, FTP_ITC.1/TLS, and FCS_TLS_EXT.1

72 The TOE implements TLS 1.2 to protect communications between the TOE and remote users' client computers (print drivers, fax drivers, and WIM HTTPS sessions). TLS client authentication is not supported. The TOE can also be configured at initial configuration to use TLS to protect communications with a remote Syslog or SMTP server.

73 The TOE supports these ciphersuites:

a) TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256

b) TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256

c) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

d) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

e) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

f) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

### 6.7.2 FCS_COP.1 (a), FCS_COP.1(b), FCS_COP.1(c) , and FCS_COP.1(g)

74 The TOE generates a self-signed Device Certificate according to FCS_CKM.1(a). Administrators may import a Device Certificate that is generated outside of the TOE.

75 To establish a session key for TLS communications, the TOE employs a Diffie-Hellman-based key establishment scheme conforming to NIST SP 800-56A Section 5.6, and a Hash DRBG. The session key is used to encrypt communications with AES 128 or AES 256 CBC:

**Table 27: TLS/HTTPS Cryptographic Functions**

| Function | SFR | Algorithm |
|---|---|---|
| **Key establishment** | FCS_CKM.1(a)<br>FCS_COP.1(b)<br>FCS_COP.1(c) | DSA KeyGen 186-4<br>KAS-FFC<br>KAS-ECC |
| **Message Authentication** | FCS_COP.1(g) | HMAC-SHA-256<br>HMAC-SHA-384<br>HMAC-SHA-512 |
| **Random number generation** | FCS_RBG_EXT.1 | Hash_DRBG_SHA256 |
| **Encryption / decryption** | FCS_COP.1(a) | AES 128 CBC<br>AES 256 CBC<br>AES 128 GCM<br>AES 256 GCM |

### 6.7.3 FCS_ITC.1/IPsec, FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, and FCS_COP.1(g)

76 The TOE employs IPsec to protect communications between the TOE and external IT entities in the operational environment. In the evaluated configuration, it is used for communications with LDAP, syslog, NTP, SMTP, and FTP servers.

77 IPsec is operated in transport mode, as set by the administrator.

78 IPsec supports automatic key exchange or automatic key exchange by IKEv1.

79 In Phase 1, peer authentication supports two types of authentication: pre-shared key authentication and digital certificate authentication.

80 The pre-shared key can be any length from 1 to 32 characters, and is composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”). Text-based pre-shared keys of 22 characters is supported. The pre-shared key is configurable with an ASCII text string, and it is conditioned using a SHA-256 hash.

81 An administrator can select whether to use main mode or aggressive mode. In the evaluated configuration, only main mode is used.

82 In IKEv1, supported DH group is 14. The value set by the administrator is used.

83 IKEv1 key lifetimes can be set by the administrator, from 300 seconds to 172,800 seconds. In the evaluated configuration, Phase 1 key lifetime is set to 86,400 seconds (24 hours), and Phase 2 lifetime is set to 28,800 seconds (8 hours).

84 As an SPD, four individual entries and one default entry of Protect can be set by an administrator. Beginning with the first entry the packet is compared, and if it matches the entry, IPsec communication is performed. If the packet does not match the first entry, subsequent entries are tested until there is a match. If no entries match the packet, the default entry will be compared, and if it does not match, the packet is discarded.

85 The TOE supports these cryptographic algorithms:

**Table 28: IPsec Cryptographic Functions**

| Function | SFR | Algorithm |
|---|---|---|
| **IKEv1** | FCS_CKM.1(a)<br>FCS_COP.1(a)<br>FCS_COP.1(b)<br>FCS_COP.1(g)<br>FCS_RBG_EXT.1 | RSA 186-4<br>AES 128 CBC<br>AES 256 CBC<br>HMAC-SHA-256<br>HMAC-SHA-384<br>HMAC-SHA-512 |
| **ESP** | FCS_COP.1(a)<br>FCS_COP.1(b)[DIM]<br>FCS_COP.1(g)<br>FCS_RBG_EXT.1 | AES 128 CBC<br>AES 256 CBC<br>HMAC-SHA-256<br>HMAC-SHA-384<br>HMAC-SHA-512 |

## 6.8 Administrative Roles

86 The Security Management Function consists of functions to 1) control operations for TSF data, 2) maintain user roles assigned to Normal Users, MFP Administrator, or MFP Supervisor to operate the Security Management Function, and 3) set appropriate default values to security attributes, all of which accord with user role privileges or user privileges that are assigned to Normal Users, MFP Administrator, or MFP Supervisor.

### 6.8.1 FMT_SMR.1

87 The TOE maintains U.NORMAL and U.ADMIN roles as described in Table 6. U.NORMAL defines the normal or non-admin users of the TOE which are permitted to use the document processing functions of the MFP and access their own data. U.ADMIN defines All TOE administrators w which includes the MFP Administrator and the MFP Supervisor. The MFP Administrator configures the TOE, manages normal users' jobs and normal users' data. The MFP supervisor sets MFP Administrators' passwords. Administrators do not initiate document processing jobs.

### 6.8.2 FMT_SMF.1, FMT_MOF.1, and FMT_MTD.1

88 The TOE provides and restricts the following management functions which can be managed over the Operation Panel or the WIM:

a) Manage user accounts including create, modify, delete users, user roles, privileges, available function lists.

b) Manage the document user list for stored documents

c) Manage the audit functions including enable/disable the audit functions and modifying the audit transfer settings

d) Query, delete and export the audit logs

e) Configure time and date settings

f) Password Management including configuring password composition, password length, and password complexity

g) Configure auto logout settings on WIM and the Operation Panel

h) Configure Authentication Failure and Account lockout timer settings

i) Modify PSTN Fax-Line Separation Stored Reception File User

j) Configure Image Overwrite

k) Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE)

l) Manage HDD cryptographic keys

m) Manage device certificates including create, query, delete, modify, upload, download certificates

n) Manage TOE trusted update

o) Configure IPsec

p) Configure SMTP over IPsec

q) Configure NTP

89 The TOE restricts modification of TSF functions and TSF data to the authorized administrator roles.

### 6.8.3 FMT_MSA.1 and FMT_MSA.3

90 Table 18 and Table 19 list the access control rules enforced by the TOE when users access the document processing functions (print, scan, copy, fax) and individual user jobs. The default behaviour to access the document data is permissive for all authenticated normal users, except for the U.ADMIN user which cannot initiate document processing functions. The TOE maintains username and available function lists data for individual users, unauthenticated users sending document print of document fax to the TOE must be identified before the TOE processes the job.

## 6.9 Trusted Operation

91 The Software Verification Function is to verify the integrity of the executable codes of the MFP Control Software, FCU Control Software and Operation Panel Control Software, and confirm that these codes can be trusted.

### 6.9.1 FPT_TST_EXT.1, FCS_COP.1(b), FCS_COP.1(c)/L1, and FCS_COP.1(c)/L2

92 During start-up, the TOE performs a series of integrity tests, that check that the hash on the executable files is correct and that the software has not been changed. The integrity tests check the hash on the software executable listed below:

**Table 29: Start-up Integrity Tests**

| Integrity test | SFR | Algorithm |
|---|---|---|
| **TPM** | FCS_COP.1(c)/L1 | SHA-1 |
| **MFP Control Software** | FCS_COP.1(b)<br>FCS_COP.1(c)/L2 | RSA 186-4<br>SHA-256 |
| **Fax Control Unit** | FCS_COP.1(c)/L1 | SHA-1 |
| **Operation Panel Software** | FCS_COP.1(b)<br>FCS_COP.1(c)/L1 | RSA 186-4<br>SHA-1 |
| **Operation Panel Applications** | FCS_COP.1(b)<br>FCS_COP.1(c)/L1 | RSA 186-4<br>SHA-1 |

93 If any steps of the integrity tests fail, a Service Call (SC) error code is displayed on the Operator Panel and the TOE becomes unavailable. In such cases, the Administrator must contact a Customer Engineer to service the TOE.

94 When all steps succeed, the TOE becomes operational.

95 Testing that the hash on the TOE software image is correct before the TOE can become operational verifies the integrity and validity of the TOE software; this is sufficient to demonstrate that the TSF is operating correctly.

### 6.9.2 FPT_TUD_EXT.1, FCS_COP.1(b), FCS_COP.1(c)/L1, and FCS_COP.1(c)/L2

96 TOE allows only the MFP Administrator to read the version of the MFP Control Software, Operation Panel Control Software, and FCU Control Software. The MFP Administrator can read these versions using the Operation Panel or WIM from the client computer.

97 The MFP Administrator can prepare for installation of updated MFP Control Software, Operation Panel Software, or FCU Control Software, by uploading an installation package from the client computer using WIM. The package contains the TOE Software and a digital signature (DS) that was created using the SERES private key. Digital signatures for trusted updates are generated outside of the TOE, by the manufacturer.

98 For MFP Control or FCU Software, the TOE performs the following verifications before the installing the package:

a) Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);

b) Verifies that the software model name matches the TOE;

c) Creates a SHA256 message digest (MD1) of the software, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.

99 For Operation Panel software, the TOE performs the following verifications before the installing the package:

a) Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);

b) Verifies that the software model name matches the TOE;

c) Creates a SHA256 message digest (MD1) of the index file, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.

d) Creates a SHA256 message digest (MD3) of the software image, uses an internal key to decrypt DS (MD4), and then verifies that MD3 = MD4.

100 The TOE performs the signature verification of the software to be updated using the encryption functions listed below when updating the software.

**Table 30: Signature Verification**

| Integrity test | SFR | Algorithm |
|---|---|---|
| **MFP Control Software** | FCS_COP.1(b)<br>FCS_COP.1(c)/L2 | RSA 186-4<br>SHA-256 |
| **Operation Panel Software** | FCS_COP.1(b)<br>FCS_COP.1(c)/L2 | ECDSA SigVer 186-4<br>SHA-256 |
| **Operation Panel Applications** | FCS_COP.1(b)<br>FCS_COP.1(c)/L2 | RSA 186-4<br>ECDSA SigVer 186-4<br>SHA-256 |

## 6.10 PSTN Fax-Network Separation

101 The Fax Line Separation Function permits only fax transmissions as input information from telephone lines so that unauthorized intrusion from telephone lines can be prevented.

### 6.10.1 FDP_FXS_EXT.1

102 The fax interface use cases are below.

a) Sending faxes

i) The TOE receives documents from client PCs via the LAN, and using the fax interface, transmits them as fax documents via the PSTN line using the ITU-T T.30 protocol.

ii) The TOE can transmit stored documents as faxes.

b) Receiving faxes

i) A remote fax machine establishes a connection to the TOE through the PSTN line using the ITU-T T.30 protocol, through which the TOE receives fax documents.

c) Fax-Line Separation

i) The fax modem accepts connections through the PSTN only if they conform to the ITU-T T.30 protocol.

ii) Data that is transmitted or received through the PSTN is fax-format, image data.

103 Other than the specified use cases, the TOE allows no other data to be transmitted on the fax line.

## 6.11 Image Overwrite

### 6.11.1 FDP_RIP.1(a)

104 During the processing of jobs, image data is stored on the HDD. When such data is no longer needed by the user or the TOE, residual data can be overwritten using the Auto Erase Memory function.

105 When enabled, the Auto Erase Memory function automatically overwrites the residual image data after each completion of the following processing jobs:

a) Copy jobs

b) Print jobs

c) Sample Print/Locked Print/Hold Print

d) Stored Print jobs (after deletion of the job)

e) Spool printing jobs

f) LAN-Fax print data

g) Faxes sent/received using remote machines

h) Scanned files sent by e-mail

i) Files sent by Scan to Folder

j) Documents sent using Web Image Monitor

k) Documents deleted from the Document Server using the Copier, Printer, Fax or Scanner functions

106 When the Auto Erase Memory function is enabled, such data is actively overwritten with values and repetition selected by the Administrator:

a) NSA: Temporary data is overwritten twice with random numbers and once with zeros.

b) DoD: Each item of data is overwritten by a random number, then by its complement, then by another random number, and is then verified.

c) Random Numbers: Temporary data is overwritten multiple times with random numbers. The number of overwrites can be selected from 1 to 9, default 3.

# 7 Rationale

## 7.1 Conformance Claim Rationale

107 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is hardcopy device, consistent with the HCDPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the HCDPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the HCDPP.

d) **Security requirements.** As shown in section 4, the security requirements are reproduced directly from the HCDPP. No additional requirements have been specified.

## 7.2 Security Objectives Rationale

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

**Table 31: Security Objectives Rationale**

| Threat/Policy/Assumptions | Rationale |
|---|---|
| T.UNAUTHORIZED_ACCESS<br>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. | O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users.<br>O.USER_I&A provides the basis for access control.<br>O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators. |
| T.TSF_COMPROMISE<br>An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces. | O.ACCESS_ CONTROL restricts access to TSF Data in the TOE to authorized Users.<br>O.USER_I&A provides the basis for access control.<br>O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators. |
| T.TSF_FAILURE<br>A malfunction of the TSF may cause loss of security if the TOE is permitted to operate. | O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected. |
| T.UNAUTHORIZED_UPDATE<br>An attacker may cause the installation of unauthorized software on the TOE. | O.UPDATE_VERIFICATION verifies the authenticity of software updates. |

| Threat/Policy/Assumptions | Rationale |
|---|---|
| T.NET_COMPROMISE<br>An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication. | O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks. |
| P.AUTHORIZATION<br>Users must be authorized before performing Document Processing and administrative functions. | O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users.<br>O.USER_I&A provides the basis for authorization.<br>O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators. |
| P.AUDIT<br>Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity. | O.AUDIT requires the generation of audit data.<br>O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users.<br>O.USER_AUTHORIZATION provides the basis for authorization. |
| P.COMMS_PROTECTION<br>The TOE must be able to identify itself to other devices on the LAN. | O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks. |
| P.STORAGE_ENCRYPTION (conditionally mandatory)<br>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. | 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)<br>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. | 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)<br>If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN. | O.FAX_NET_SEPARATION requires a separation between the PSTN fax line and the LAN. |

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

**Table 32: Security Objectives Rationale**

## 7.3 Security Assurance Requirements rationale

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities throughout the PP are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.

# Annex A: Extended Components Definition

109 This annex reproduces the HCDPP Appendix A.9 extended components definition.

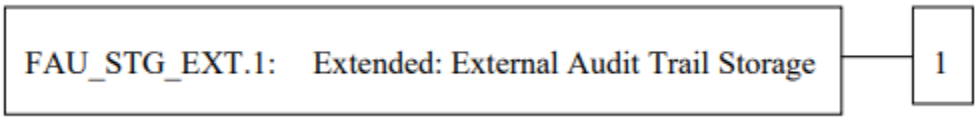
## Security Audit (FAU)

### External Audit Trail Storage (FAU_STG_EXT)

#### Family Behavior

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

#### Component levelling




FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management:
The following actions could be considered for the management functions in FMT:

a) The TSF shall have the ability to configure the cryptographic functionality.

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

**FAU_STG_EXT.1 Extended: Protected Audit Trail Storage**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FAU_GEN.1 Audit data generation<br>FTP_ITC.1 Inter-TSF Trusted Channel |
| FAU_STG_EXT.1.1 | The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC. |

Rationale:
The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

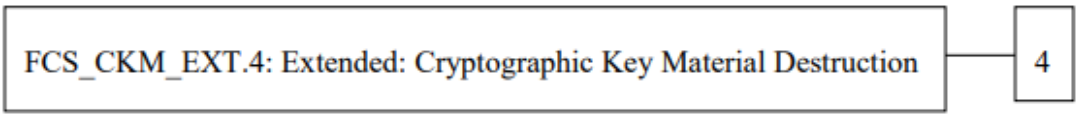
# Cryptographic Support (FCS)

## Cryptographic Key Management (FCS_CKM_EXT)

### Family Behavior

This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

### Component levelling




FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen

| **FCS_CKM_EXT.4** | **Extended: Cryptographic Key Material Destruction** |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM_EXT.4.1 | The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed. |

Rationale:
Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

## HTTPS selected (FCS_HTTPS_EXT)

### Family Behavior

Components in this family define the requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

### Component levelling


FCS_HTTPS_EXT.1 HTTPS selected, requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Failure of HTTPS session establishment.

### FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement the HTTPS protocol using TLS as specified in FCS_TLS_EXT.1.

Rationale:

HTTPS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

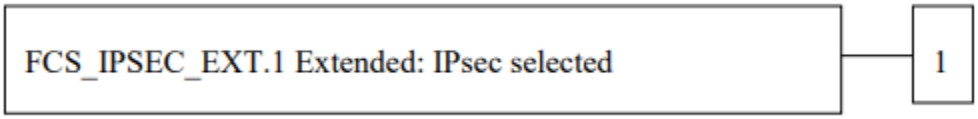
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

## IPsec selected (FCS_IPSEC_EXT)

### Family Behavior

This family addresses the requirements for protecting communications using IPsec.

### Component levelling




FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management actions foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
b) Failure to establish an IPsec SA.

### FCS_IPSEC_EXT.1 Extended: IPsec selected

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition<br>FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) |
| FCS_IPSEC_EXT.1.1 | The TSF shall implement the IPsec architecture as specified in RFC 4301. |
| FCS_IPSEC_EXT.1.2 | The TSF shall implement [selection: tunnel mode, transport mode]. |
| FCS_IPSEC_EXT.1.3 | The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it. |
| FCS_IPSEC_EXT.1.4 | The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106]. |
| FCS_IPSEC_EXT.1.5 | The TSF shall implement the protocol: [selection: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]]. |

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: IKEv1, IKEv2] protocol uses the cryptographic algorithms [selection: AES-CBC-128, AES_CBC-192 AES-CBC-256 as specified in RFC 3602, AES-GCM-128, AES-GCM-192, AES-GCM-256 as specified in RFC 5282, no other algorithm].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: IKEv2 SA lifetimes can be established based on [selection: number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]; IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]]

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)), [assignment: other DH groups that are implemented by the TOE], no other DH groups].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: RSA, ECDSA] algorithm and Pre-shared Keys.

Rationale:
IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

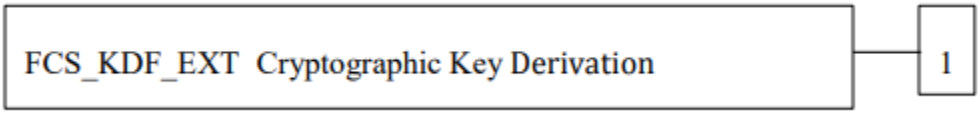
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection: 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)].

## Cryptographic Key Derivation (FCS_KDF_EXT)

### Family Behavior

This family specifies the means by which an intermediate key is derived from a specified set of submasks.

### Component levelling




FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen

### FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),<br><br>[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)] |
| FCS_KDF_EXT.1.1 | The TSF shall accept [selection: a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask] to derive an intermediate key, as defined in [selection: NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV. |

## Cryptographic Operation (FCS_KYC_EXT)

### FCS_KYC_EXT Cryptographic Operation (Key Chaining)

### Family Behavior

This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

### Component levelling


FCS_KYC_EXT Key Chaining, requires the TSF to maintain a key chain and specifies the characteristics of that chain.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

### FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components

Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping), FCS_SMC_EXT.1 Extended: Submask Combining, FCS_COP.1(i) Cryptographic operation (Key Transport), FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1(f) Cryptographic operation (Key Encryption)].

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: one, using a submask as the BEVor DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s): [selection: key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)]] while maintaining an effective strength of [selection: 128 bits, 256 bits].

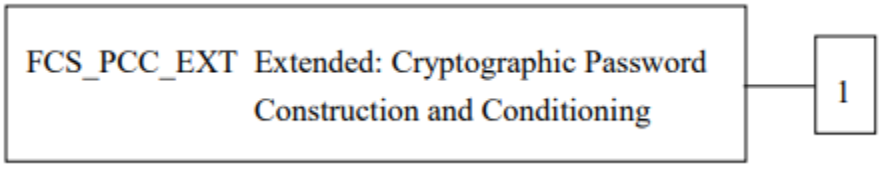
Rationale:
Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

## Cryptographic Password Construction and Conditioning (FCS_PCC_EXT)

### Family Behavior

This family ensures that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

### Component levelling




FCS_PCC_EXT.1 Cryptographic Password Construction and Conditioning, requires the TSF to accept passwords of a certain composition and condition them appropriately.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

### FCS_PCC_EXT.1 Extended: Cryptographic Password Construction and Conditioning

Hierarchical to: No other components

Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

FCS_PCC_EXT.1.1 A password used to generate a password authorization factor shall enable up to [assignment: positive integer of 64 or more] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: other supported special characters]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: SHA-256, SHA384, SHA-512]], with [assignment: positive integer of 1000 or more] iterations, and output cryptographic key sizes [selection: 128, 256] that meet the following: [assignment: PBKDF recommendation or specification].

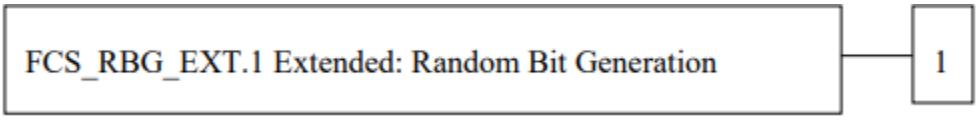
## Random Bit Generation (FCS_RBG_EXT)

### FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

### Family Behavior

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

### Component levelling




FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen

### FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011, NIST SP 800-90A using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source(s), [assignment: number of hardware-based sources] hardware-based noise source(s)] with a minimum of [selection: 128 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

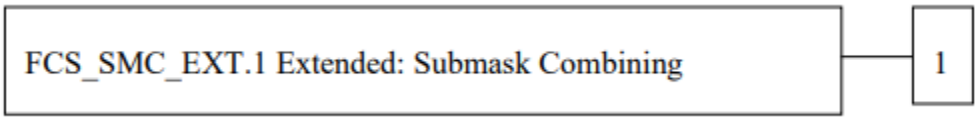
Rationale:
Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.
This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

## Submask Combining (FCS_SMC_EXT)

### Family Behavior

This family defines the means by which submasks are combined, if the TOE supports more than one submask being used to derive or protect the BEV.

### Component levelling




FCS_SMC_EXT.1 Submask combining requires the TSF to combine the submasks in a predictable fashion

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management actions foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

### FCS_SMC_EXT.1 Extended: Submask Combining

Hierarchical to: No other components

Dependencies: FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: exclusive OR (XOR), SHA-256, SHA-512] to generate an intermediary key or BEV.

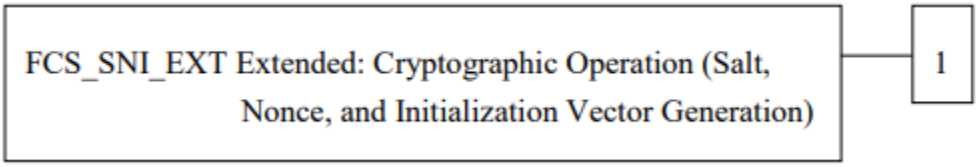
Rationale:
Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV.
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

## Salt, Nonce, and Initialization Vector Generation (FCS_SNI_EXT)

### Family Behavior

This family ensures that salts, nonces, and IVs are well formed.

### Component levelling




FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation), requires the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.

Management:
The following actions could be considered for the management functions in FMT:
a) No specific management functions are identified

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

### FCS_SNI_EXT.1 Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

Hierarchical to: No other components

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [ CBC: IVs shall be non-repeating, CCM: Nonce shall be non-repeating, XTS: No IV. Tweak

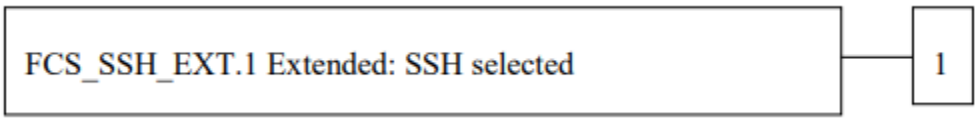
values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer, GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.].

## SSH selected (FCS_SSH_EXT)

### Family Behavior

The component in this family addresses the ability for a server to offer SSH to protect data between a client and the server using the SSH protocol.

### Component levelling




FCS_SSH_EXT.1 SSH selected, requires the SSH protocol implemented as specified.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) Failure of SSH session establishment

### FCS_SSH_EXT.1 Extended: SSH selected

Hierarchical to: No other components

Dependencies: No dependencies

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [selection: 4251, 4252, 4253, 4254, and [selection: 5656, 6668, no other RFCs].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption

| | |
|---|---|
| | algorithms: [assignment: AES-CBC-128, AES-CBC-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].]. |
| FCS_SSH_EXT.1.5 | The TSF shall ensure that the SSH transport implementation uses [selection: SSH_RSA, ecdsa-sha2-nistp256] and [selection: PGP-SIGN-RSA, PGP-SIGNDSS, ecdsa-sha2-nistp384, no other public key algorithms,] as its public key algorithm(s). |
| FCS_SSH_EXT.1.6 | 6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-512]. |
| FCS_SSH_EXT.1.7 | The TSF shall ensure that diffie-hellman-group14-sha1 and [selection: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, no other methods] are the only allowed key exchange method used for the SSH protocol. |

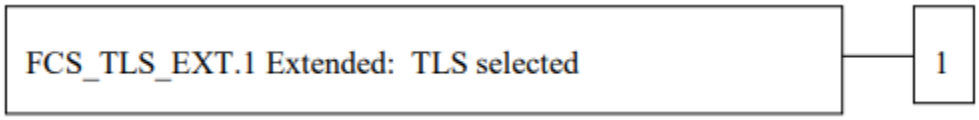
Rationale:
SSH is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

## TLS selected (FCS_TLS_EXT)

### Family Behavior

This family addresses the ability for a server and/or a client to use TLS to protect data between a client and the server using the TLS protocol.

### Component levelling




FCS_TLS_EXT.1 TLS selected, requires the TLS protocol implemented as specified.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) Failure of TLS session establishment

### FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to: No other components

Dependencies: No dependencies

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional ciphersuites:

[selection:

- None
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384].

Rationale:
TLS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

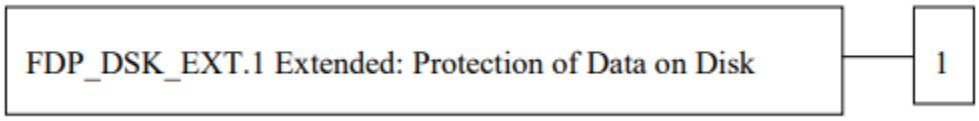
# User Data Protection (FDP)

## Protection of Data on Disk (FDP_DSK_EXT)

### Family Behavior

This family is to mandate the encryption of all protected data written to the storage.

### Component levelling




FDP_DSK_EXT.1 Extended: Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Non-volatile Storage Devices in order to avoid storing these data in plaintext on the devices.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

### FCS_DSK_EXT.1 Extended: Protection of Data on Disk

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption) |
| FDP_DSK_EXT.1.1 | The TSF shall [selection: perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data. |
| FDP_DSK_EXT.1.2 | The TSF shall encrypt all protected data without user intervention. |

Rationale:
Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

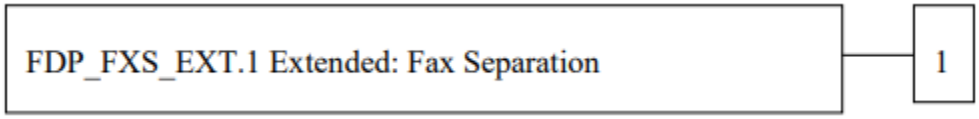
This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

## Fax Separation (FDP_FXS_EXT)

### Family Behavior

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

### Component levelling




FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

**FCS_FXS_EXT.1 Extended: Fax separation**

Hierarchical to: No other components

Dependencies: No dependencies

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

Rationale:
Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.

This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

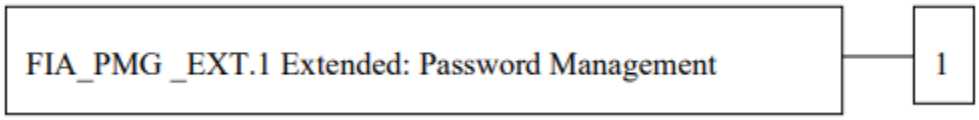
# Identification and Authentication (FIA)

## Password Management (FIA_PMG_EXT)

### Family Behavior

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

### Component levelling




FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

**FIA_PMG_EXT.1 Extended: Password Management**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

c) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]];

d) Minimum password length shall be settable by an Administrator and have the capability to require passwords of 15 characters or greater.

Rationale:
Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.
This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

## Pre-Shared Key Composition (FIA_PSK_EXT)

### Family Behavior

This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

### Component levelling


FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

**FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition**

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [selection: [assignment: other supported lengths], no other lengths];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”

  ).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: SHA-1, SHA-256, SHA-512, [assignment: method of conditioning text string]] and be able to [selection: use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1].

Rationale:
Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.
This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

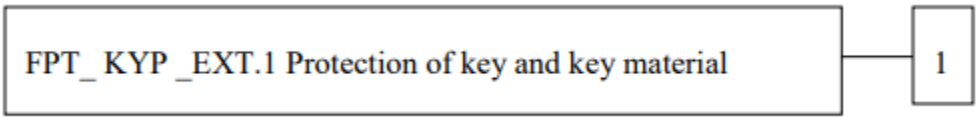
# Protection of the TSF (FPT)

## Protection of Key and Key Material (FPT_KYP_EXT)

### Family Behavior

This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

### Component levelling




FPT_KYP_EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

Management: FPT_SKP_EXT.1
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit: FPT_SKP_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

| **FPT_KYP_EXT.1** | **Extended: Protection of Key and Key Material** |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_KYP_EXT.1.1 | 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, and not store any such plaintext key on a device that uses the key for its encryption. |

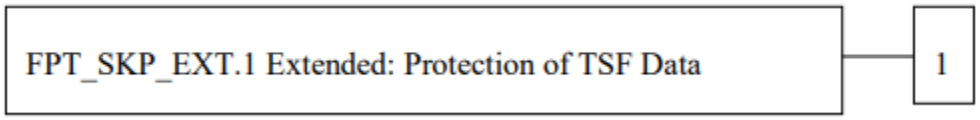
Rationale:
Protection of Key and Key Material is to ensure that no plaintext key or key material are written to non-volatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.
This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

## Protection of TSF Data (FPT_SKP_EXT)

### Family Behavior

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

### Component levelling




FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

| **FPT_SKP_EXT.1** | **Protection of TSF Data** |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No other components. |
| FPT_SKP_EXT.1.1 | The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys. |

Rationale:
Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.
This extended component protects the TOE by means of strong authentication using Preshared Key, and it is therefore placed in the FPT class with a single component.

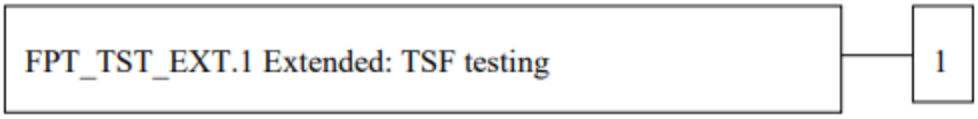
## TSF Self-Test (FPT_TST_EXT)

**FPT_TST_EXT.1 TSF Testing**

### Family Behavior

TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

### Component levelling




FPT_TST_EXT.1 TSF Self-Test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management:
The following actions could be considered for the management functions in FMT:
a) No management functions.

Audit:
The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen.

**FPT_TST_EXT.1 Extended: TSF testing**

Hierarchical to: No other components.

Dependencies: No other components.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

Rationale:
TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing. This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

## Trusted Update (FPT_TUD_EXT)

### Family Behavior

This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware and/or software.

### Component levelling


FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

Management:
The following actions could be considered for the management functions in FMT:
a) There are no management actions foreseen

Audit:
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) There are no auditable events foreseen

| **FPT_TUD_EXT.1** | **Extended: Trusted Update** |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), or FCS_COP.1(c) Cryptographic operation (Hash Algorithm)]. |
| FPT_TUD_EXT.1.1 | The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software |
| FPT_TUD_EXT.1.2 | The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software. |
| FPT_TUD_EXT.1.3 | The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: digital signature mechanism, published hash] prior to installing those updates. |

Rationale:
Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.
This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

# Annex B: Security Assurance Requirements

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 22 provides evaluative activities required to address the threats identified in Section 0 of this PP.

## 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.

## 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.

### ADV_FSP.1 Basic functional specification

The functional specification describes the TSF Interfaces (TSFIs). At the level of assurance provided by this PP, it is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users (to include administrative users), at this assurance level there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. The activities for this family for this PP should focus on understanding the interfaces presented in the TSS in response to the functional requirements, and the interfaces presented in the AGD documentation. No additional “functional specification” document should be necessary to satisfy

the assurance activities specified. The interfaces that need to be evaluated are characterized through the information needed to perform the 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.

**Assurance activity**:

TSS:

The evaluator shall confirm identifiable external interfaces from guidance documents and examine that TSS description identifies all the interfaces required for realizing SFR.

The evaluator shall confirm identification information of the TSFI associated with the SFR described in the TSS and confirm the consistency with the description related to each interface.

The evaluator shall check to ensure that the SFR defined in the ST is appropriately realized, based on identification information of the TSFI in the TSS description as well as on the information of purposes, methods of use, and parameters for each TSFI in the guidance documents

The assurance activities specific to each SFR are described in Section 5 and the evaluator shall perform evaluations by adding to this assurance component.

# Class AGD: Guidance Documents

The guidance documents will be provided with the developer's security target. Guidance must include a description of how the administrator verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an administrator.

Guidance must be provided for every Operational Environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment; and
- instructions to manage the security of the TOE as a product and as a component of the larger Operational environment.

Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the assurance activities specified in Section 5.

## 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 ser-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.

**Assurance activity:**

Operational Guidance:

The contents of operational guidance are confirmed by the assurance activities in Section 5 and the TOE evaluation in accordance with the CEM.

The evaluator shall check to ensure that the following guidance is provided:

Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the transition from the maintenance mode to the normal Operational Environment.

**Application note:**

During evaluation, the TOE returns to its evaluation configuration. In the field, the TOE may return to the configuration that was in force prior to entering maintenance mode.

## 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.

# Class ALC: Life-cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

## ALC_CMC.1 Labelling of the TOE

This component is targeted at identifying the TOE such that it can be distinguished from other products or 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.

**Assurance activity:**

Operational Guidance:

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

## ALC_CMS.1 TOE CM coverage

Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance 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.

**Assurance activity:**

Operational Guidance:

The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

# Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces as constrained by the availability of design information presented in the TSS. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

## ATE_IND.1 Independent testing - Conformance

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 5 are being met, although some additional testing is specified for SARs in Section 7. The Assurance Activities identify the minimum testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage 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. |

**Assurance activity:**

Test:

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the product models to be tested, and for those product models not included in the test plan but included in the ST, the test plan provides a justification for not testing the models. This justification must address the differences between the tested models and the untested models, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. In case the ST describes multiple models (product names) in particular, the evaluator shall consider the differences in language specification as well as the influences, in which functions except security functions such as a printing function, may affect security functions when creating this justification. If all product models claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each product model to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each model either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include the goal of the particular procedure, the test steps used to achieve the goal, and the expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

## Class AVA: Vulnerability Assessment

For the first generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing 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.

Assurance activity:

Test:

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in printing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report.

For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability.

For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.