Canon imageRUNNER ADVANCE DX 48945KG/48935KG/48925KG/ 4845F/4845i/4845/ 4835F/4835i/4835/ 4825F/4825i/4825 with Fax & PDL

Security Target

Version 1.02
2022/07/27

Canon Inc.

This document is a translation of the evaluated and certified security target written in Japanese.

Table of Contents

Trademark Notice

- Canon, the Canon logo, imageRUNNER, imageRUNNER ADVANCE, imageRUNNER ADVANCE DX, imagePRESS,imagePRESSLite are trademarks or registered trademarks of Canon Inc.
- Microsoft, Windows, Windows Server 2012, Windows 10, Microsoft Edge are trademarks or registered trademarks of Microsoft Corporation in the U.S. and other countries.
- All names of companies and products contained herein are trademarks or registered trademarks of the respective companies.

1 ST introduction

1.1 ST reference

This section provides the Security Target (ST) identification information.

ST name:	Canon imageRUNNER ADVANCE DX 48945KG/48935KG/48925KG/4845F/4845i/4845/4835F/4835i/4835/4825F/4825i/4825 with Fax & PDL Security Target
Version:	1.02
Issued by:	Canon Inc.
Date of Issue:	2022/07/27

1.2 TOE reference

This section provides the TOE identification information.

TOE name:	Canon imageRUNNER ADVANCE DX 48945KG/48935KG/48925KG/4845F/4845i/4845/4835F/4835i/4835/4825F/4825i/4825 with Fax & PDL
Version:	202

This TOE consists of the MFP body, firmware, fax, and page description language processing (see Table 3). The TOE can be confirmed by the identification information of the manufacturer name, the identification information of the MFP body, the identification information of the firmware, the identification information of the fax, and the identification information of the page description language processing shown in Table 1 below.

Table 1 - The identification information of the TOE

Type of identification information	Identification information
manufacturer name	[Canon]
MFP body	One of [iR-ADV 4845], [iR-ADV 4835], [iR-ADV 4825]
firmware	[202]
fax	[Super G3 FAX Board-BH]
page description language processing	[PCL] and [PS]

1.3 TOE overview

1.3.1 TOE Type

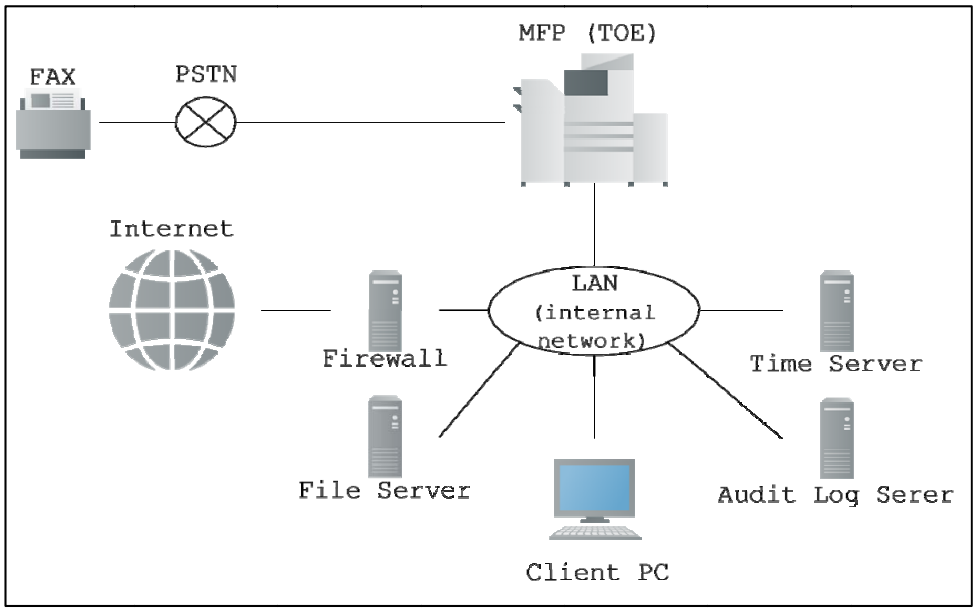
The TOE is an MFP having a print function, a scan function, a copy function, a fax function, and a Storage and retrieval function.

1.3.2 Usage and Major Security Features of the TOE

The TOE is an MFP having a print function, a scan function, a copy function, a fax function, and a Storage and retrieval function. In order to protect these documents from unauthorized alteration and disclosure, the TOE has a user authentication function that identifies and authenticates the user, an access control function for document data and functions based on authority, a PSTN fax-network separation function, an SSD encryption function of the TOE embedded SSD, a LAN data protection function and a signature verification/generation function that protect network communications, a self-test function that checks the integrity of TSF execution codes at startup, an audit log function that monitors the use of the TOE security function and sends the monitoring results (audit logs) to an audit log server, and stores audit logs internally in the TOE, a reliable update function that update execution code while confirming authenticity of TOE's upugrade execution code, and a management function that limits security settings to administrators.

Figure 1 shows the assumed operational environment when using the functions of the TOE.

Figure 1 Operational environment of the TOE



1.3.3 Required Non-TOE Hardware and Software

The non-TOE hardware and software configurations in Figure 1 are shown below.

1) Time Server

The TOE communicates with SNTP-enabled servers (This operation assumes Windows Server 2012 R2 Standard Edition.) to obtain accurate time.

2) Audit Log Server

An external audit log server (This operation assumes SMB servers using Windows Server 2012 R2 Standard Edition) for storing TOE-generated audit logs. The audit log server obtains the audit log in SMB.

3) Client PC

Generic PC running Windows 10. A user having an account in TOE can send a print job to TOE by installing and setting a printer driver (In this operation, the printer driver described in Table 2 is assumed.)

corresponding to this TOE. In addition to printing, administrators can access TOE through a web browser (Microsoft Edge is assumed in this case) to use management capabilities of the TOE.

Table 2 - Printer Driver

Printer Driver
Generic Plus UFRII Printer Driver V2.50 (Japanese name: Generic Plus LIPSLX Printer Driver V2.50)
Generic Plus PS3 Printer Driver V2.50
Generic Plus PCL6 Printer Driver V2.50

4) File Server

Storage space when sending scanned documents with TOE. This operation assumes an SMB server using Windows Server 2012 R2 Standard Edition.

5) Firewall

A device that protects the internal network to which a TOE connects from unauthorized access from the Internet environment. This indicates that the environment satisfies the Usage Assumptions A. NETWORK of this TOE and does not assume any specific product.

6) Fax

To transmit and receive a fax image via TOE and PSTN. Faxes compatible with the G3 standard are expected.

1.4 TOE description

1.4.1 Physical scope of the TOE

TOE is a digital multifunction device and guidance.

The digital multifunction peripheral constituting the TOE is an MFP body in which the firmware of the designated Controller Version operates, and has a fax function (in the case of an option, a fax board is installed) and page description language processing (If optional, purchase PCL option, PS option to enable PCL/PS feature). As Table 3- Product Line-up , fax board, PCL option, and PS option need to procure the appropriate options to match the selling name in the selling area.

Table 3 - Product Line-up

MFP Body (Controller Version 202)	Sales area	fax board	PCL option[1]	PS option[1]
imageRUNNER ADVANCE DX 48945KG imageRUNNER ADVANCE DX 48935KG imageRUNNER ADVANCE DX 48925KG	Korea	Super G3 FAX Board-BH1	PCL Printer Kit-CC1	PS Printer Kit-BG1
imageRUNNER ADVANCE DX 4845F imageRUNNER ADVANCE DX 4835F imageRUNNER ADVANCE DX 4825F	Japan	Not required (standard	PCLエミュレーション拡張キット・AS1	PS拡張キット・BF1

[1] The purchase of the PCL option/PS option provides an MFP with the PCL/PS processing function of the firmware enabled. There are no shipments for this option.

		equipment)		
imageRUNNER ADVANCE DX 4845i imageRUNNER ADVANCE DX 4835i imageRUNNER ADVANCE DX 4825i	Americas	Super G3 FAX Board-BH1	Not required (standard equipment)	Not required (standard equipment)
	Asia/Taiwan (except 4825i)	Super G3 FAX Board-BH1	Not required (standard equipment)	PS Printer Kit-BG1
imageRUNNER ADVANCE DX 4845 imageRUNNER ADVANCE DX 4835 imageRUNNER ADVANCE DX 4825	Asia/India/Korea	Super G3 FAX Board-BH1	PCL Printer Kit-CC1	PS Printer Kit-BG1

*The Korean government model differs from other models in terms of the name of the product. The difference from similar model names is that there is a "9" in the middle of the four-digit number and KG is added after the number.

*F: FAX (with fax board/F model), Only Model F is available in Japan.

*i: PDL (optional PDL enabled/i model). The effective PDL depends on the sales area.

A service engineer dispatched from a sales company attaches a fax board to the MFP body, installs firmware (not directly distributed to consumers) of a designated controller version brought by the service engineer, sets page description language processing (PCL, PS) to a valid state according to purchased license information (not directly distributed to consumers), and provides the MFP body to consumers.

Therefore, the delivered item is an MFP body delivered after the above operation, and is identified by each identification information (MFP front panel MFP name and MFP operation panel MFP body, firmware, FAX, and page description language processing) described in Table 1.

The following guidance contained in the TOE is available at the direction of the service engineer. The guidance will be distributed to TOE consumers in a PDF file via the website (https://oip.manual.canon/). When accessing the website, select your region of purchase and select the appropriate model of CC certified product to obtain the guidance below.

(Japanese name)

- imageRUNNER ADVANCE DX 4800 シリーズ用 Protection Profile for Hardcopy Devices 対応セキュリティー設定 アドミニストレーターガイド [USRMA-7637-00 20220610]
- imageRUNNER ADVANCE DX 4845F / 4835F / 4825F ユーザーズガイド（CC 認証参照用） [USRMA-7638-00]
- imageRUNNER ADVANCE DX 4800 シリーズ用 ACCESS MANAGEMENT SYSTEM アドミニストレーターガイド（CC 認証参照用） [USRMA-7639-00]

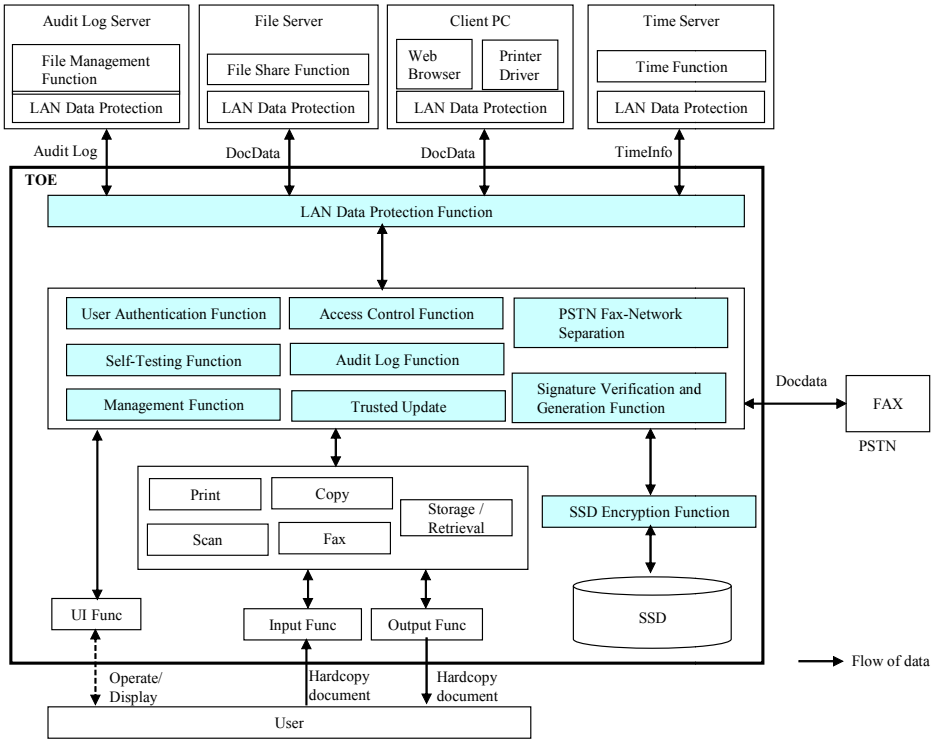
(English name)

- imageRUNNER ADVANCE DX 4800 Series Protection Profile for Hardcopy Devices adaptive Security Settings Administrator Guide [USRMA-7640-00 20220610]
- imageRUNNER ADVANCE DX 4845i / 4835i / 4825i User's Guide (for CC certification reference) [USRMA-7641-00] *USE Version
- imageRUNNER ADVANCE DX 4800 series ACCESS MANAGEMENT SYSTEM Administrator Guide (for CC certification reference) [USRMA-7642-00] *USE Version
- imageRUNNER ADVANCE DX 4845i / 4845 / 4835i / 4835 / 4825i / 4825 User's Guide (for CC certification reference) [USRMA-7643-00] *APE Version
- imageRUNNER ADVANCE DX 4800 series ACCESS MANAGEMENT SYSTEM Administrator

1.4.2 Logical scope of the TOE

The logical scope of the TOE is shown in Figure 2 TOE Logical Boundary (Excluding users, file servers, audit log servers, client PCs, faxes, and time servers). The security functions of the TOE are shown in color.

Figure 2 TOE Logical Boundary



TOE has the following digital multifunction machine functions.

- Print function

  This function prints an electronic document in a digital composite machine or an electronic document transmitted from a client PC on paper.

- Scan function

  This function transmits an electronic document generated by scanning a paper document to a file server in TIFF or PDF file format.

- Copy function

  This function duplicates a paper document by scanning and printing the paper document.

- Fax function

  Fax Transmission function

This function faxes an electronic document generated by scanning a paper document through the PSTN.

Fax Reception function

This function receives an electronic document via the PSTN. When receiving a fax, the file is saved in the Inbox (system box) without being printed.

- Document Storage and Retrieval function

  Document management function of the advanced box and the system box. A document loaded by a scanner can be saved as an image in the personal space of the advanced box. You can rename, retrieve (Print, send (system box documents only)), or delete an electronic document stored in your personal space or system box.

The TOE has the following general functions.

- UI Function

  The ability for the user to operate the TOE using the operation panel, and the ability for the TOE to display a screen on the operation panel.

  It also has a remote UI function for performing TOE operation and management through a network by browser operation of a client PC.

- Output Function

  The ability of the TOE to print paper documents.

- Input Function

  The ability of TOE to scan paper documents.

The TOE has the following security functions.

- User Authentication Function

  Performs authentication on the user, to prevent any unauthorized access to the TOE. User authentication requires the user to enter a user name and password when operating from the operation panel or the remote UI, and confirms that the user is an authenticated user. The user name is authenticated through the printer driver before accepting a job from the printer driver. Verification of user information supports internal authentication to authenticate within the TOE. Give the authenticated user the privileges previously assigned to the user. When authentication is performed, the inputted password character is displayed by a specific character. It has a function of restricting access by a defined rule when authentication fails, and a function of automatically logging out when no operation state continues after authentication.

- Access Control Function

  Restrict access to jobs, electronic documents, and features based on role.

- PSTN Fax-Network Separation

  To prevent the intrusion into a LAN by limiting the use of a PSTN to a fax function.

- SSD Encryption Function

  A TOE built-in SSD is taken away and connected to another body or a PC, and all data stored in the TOE built-in SSD is encrypted by an encryption chip built in the digital multifunction device body to cope with the threat of reading data recorded in the SSD. The key used for encryption is generated in the RAM area of the encryption chip when the power of the TOE is turned on, and is used only in the encryption chip, and is managed so as not to be taken out to the outside. The encryption key becomes unnecessary and erased when the power of the TOE is turned off.

- LAN Data Protection Function

To encrypt LAN data by IPSec or TLS as a sniffing countermeasure. IPsec is used when connecting to an external device and a remote UI, and TLS is also available when an administrator connects to the remote UI. The pre-shared key and the server private key are encrypted and stored on the TOE embedded SSD and protected. The key generated during communication is generated in the RAM area of the TOE and is erased when the power of the TOE is turned off.

- Signature Verification and Generation Function

  It has a function of verifying/generating a digital signature for verifying the integrity of encrypted communication of LAN data.

- Self-Testing Function

  At boot time, verify firmware integrity with signature verification.

- Audit Log Function

  An audit log is generated with the user name of the operated user and the set time so that the operation of the unit and the operation of the user can be audited, and is stored in the TOE built-in SSD. The time is recorded using the management function or the exact date and time synchronized with the time server. All saved audit logs can only be browsed by the administrator via the remote UI. However, even an administrator cannot change the audit log. The audit log is stored in an audit log server using protected communication. There is a limit on the number of audit logs in the TOE embedded SSD, and if the number of audit logs exceeds the maximum number of retention, the oldest audit log is deleted and a new audit log is retained.

- Trusted Update Function

  When updating the TOE firmware, it has a function of verifying the firmware by version display or digital signature in order to confirm that the correct firmware is used.

- Management Function

  User management functions for registering and deleting users and roles and device management functions for properly operating various security functions, both of which are restricted to administrators only

1.5 Terms and Abbreviations

For terms used in this ST that are defined in CC and PP that are claimed to be compliant in Section 2, Follow the definition. Definitions of other terms are given in Table 4.

Table 4 - Terms and Abbreviations

Terms / Abbreviations	Description
Multi-Function Product (MFP)	A machine which incorporates the functionality of multiple devices in one, such as copier, fax, printer, and Universal Send, and containing a large capacity SSD to facilitate such capabilities.
Control software	Software that runs on the hardware of the device, and controls security functions.
PDL	It is a page description language expressing print contents, and there are various types. The print function converts print data expressed in the corresponding page description language and prints the generated image on paper.
Control panel	One of the hardware elements of the MFP, consisting of a touch panel and operation keys, which provides the interface for operation of the MFP.

Terms / Abbreviations	Description
Remote UI	An interface that provides access to the MFP from a Web browser via the LAN, to allow the acquisition of operating status, perform job operations or BOX operations, and making various settings. This interface is only available to administrators.
SSD	A nonvolatile storage device built into a digital multifunction device. Firmware and protected assets are stored.
Roles	A user's permission used by the access control function and each user is associated with one role. In addition to the predefined default roles, it is possible to create new roles as custom roles that modify the access restrictions determined by the default roles. The default role has the following roles Administrator/Power User/General User/Limited User/Guest User The Administrator role indicates the permission to use management functions (administrative permission). In this ST, a custom role is defined based on the Administrator role to which the U.ADMIN with the administrative permission and the General User to which the U.NORMAL without the administrative permission.
Administrator	User assigned the Administrator role and has administrative privileges. Equivalent to U.ADMINISTRATOR defined in the PP.
General user	U.NORMAL as defined in PP. Belong to a custom role that is created from a General User role and that does not have administrative privileges.
Fax owner	A user who is authorized by the administrator to access the Fax/I-Fax Inbox among the U.NORMAL defined in PP. Belong to a custom role that is created from a General User role and that does not have administrative privileges.
Authenticated users	All TOE-authenticated users, including administrators
Jobs	When a user uses the functions of the TOE to execute an operation on a document, a Job is the intended document data combined with the user instructions for processing those data. The operations that can be performed on a document are: Scan, Print, Copy, Fax TX, Store, and Delete. The processing phases for a Job issued by the user are: generation, execution, and completion.
Image file	Image data generated in the MFP by reading, printing, receiving, etc.
Temporaly image file	An image file that is generated during a job, such as copy/print, and becomes unnecessary when the job is completed.
Document data	User data processed within the MFP, consisting of image files and print setting.
Mail Box	Whether a general user feeds data to the MFP directly, or specifies a document for printing from a PC, data can be stored here to be printed later.
Advancesd Box	To provide an area for storing an electronic document read from a scanner in a digital multifunction device and capable of printing the stored electronic document. There is a private space for each user and a shared space for all users to access. *This TOE does not use shared space.

Terms / Abbreviations	Description
Firewall	Device or system designed to protect the internal LAN against threats from the Internet.
Time server	Server that uses the Network Time Protocol to provide the accurate time over the Internet.
File server	A file server that uses the SMB protocol to share folders over the LAN and control file storage and access
Audit log server	A server that stores audit log files that TOE outputs over a LAN using the SMB protocol.
[Print]	A button on the control panel that activates the function to operate on-hold print jobs.
[Copy]	A button on the control panel that activates the Copy function.
[Fax]	A button on the control panel that activates the Fax function.
[Scan and Send]	A button on an operation panel that loads a paper document and activates the function to send the loaded electronic document to a file server.
[Scan and Store]	A button on the control panel that activates the ability to import paper documents and save them to an advanced box.
[Access Stored Files]	A button on the control panel that allows the user to access files stored in a Mail Box/Inbox.
[Fax/I-Fax Inbox]	A button on the operation panel that activates the function for operating electronic documents saved in the system box where received fax documents are saved.

2 Conformance claims

2.1 CC Conformance claims

This ST and TOE claim CC compliance with below.

This ST conforms to the following Common Criteria (CC).

- Common Criteria version: Version 3.1 Release 5
- Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 PP claim, Package claim

This ST and TOE claim exact conformance to the following PP.

- Title: Protection Profile for Hardcopy Devices
  Version: 1.0 dated September 10, 2015
- Errata: Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

2.3 SFR Packages

In this ST, no package claims compliance.

2.4 Conformance rationale

The TOE conforms the following requirements defined in PP and is Exact Conformance as required by PP. Therefore, the TOE type is consistent with PP.

- Required Uses
  Printing, Scanning, Copying, Network communications, Administration
- Conditionally Mandatory Uses
  PSTN faxing, Storage and retrieval, Field-Replaceable Nonvolatile Storage
- Optional Uses
  Internal Audit Log Storage

3 Security Problem Definition

3.1 TOE Users

TOE users are defined in the following two user categories.

Table 5 -TOE Users

Designation	Category 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

3.2 Assets

Two asset classifications are defined for assets.

Table 6 - Assets

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

3.2.1 User Data

User data are classified into the following two types.

Table 7 - User Data

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

3.2.2 TSF Data

TSF data are classified into the following two types.

Table 8 - TSF Data

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

TSF Data handled in this TOE are shown below.

Table 9 - Realization of TSF Data

Type	TSF Data	Description	Stored in
D.TSF.PROT	User name	User identification information used by the user identification and authentication function.	SSD
	Role	Used by access restriction functions to restrict the functions that each user can use.	SSD
	Lockout policy settings	Settings for the lockout function, such as number of attempts before lockout and the lockout time.	SSD
	Password policy settings	Policy for the password for user authentication, such as minimum password length, allowed characters, and combination of character types.	SSD
	Auto Reset Time setting	Timeout period before a user logged in from the operation panel or the remote UI is automatically logged out when the user is idle.	SSD
	Date/Time setting	Specifies the date and time that is set.	RTC
	IPSec settings	Settings for the LAN Data Protection function.	SSD
	TLS settings	Settings for the LAN Data Protection function, including the settings to enable or disable the LAN Data Protection function.	SSD
	Audit log export settings	Configuration information for sending audit logs to external IT equipment	SSD
	Time server setting	for synchronizing TOE time and date with external IT equipment	SSD
D.TSF.CONF	Password	Password used to authenticate the user in the User Identification and Authentication function.	SSD
	SSD encryption key	Encryption key used for SSD encryption function	RAM in the encryption chip
	Key Seed	The internal state of DRBG and the seed value used for AES encryption key generation.	FLASH memory in the encryption chip
	LAN Data Protection Encryption Key	Encryption key used for LAN data protection function.	SSD
	Audit log	An operational record generated by the audit logging facility. It includes the date and time, user name, result, operation contents, etc.	SSD

3.3 Threats

Show threats in Table 10.

Table 10 - Threats

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

3.4 Organizational Security Policies

Show Organizational Security Policies in Table 11.

Table 11- Organizational Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	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.

3.5 Assumptions

Show Assumptions in Table 12.

Table 12 - Assumptions

Assumption	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.

A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4 Security Objectives

4.1 Security Objectives for the Operational environment

Show Security Objectives for the Operational environment in Table 13.

Table 13- Security Objectives for the Operational environment

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

5 Extended components definition

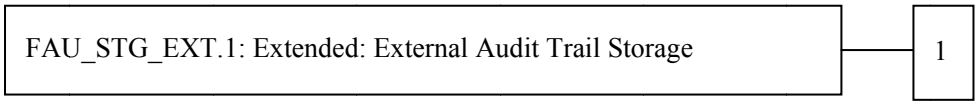
This ST defines the following security function requirements. All of these extension components are defined in the PP specified in Section 2.2.

5.1 FAU_STG_EXT Extended: External Audit Trail Storage

Family behaviour:

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

Component leveling:



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:

- 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:

- 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,
	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.1.

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.

5.2 FCS_CKM_EXT Extended: Cryptographic Key Management

Family behaviour:

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

Component leveling:

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:

- 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:

- There are no auditable events foreseen.

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.

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.

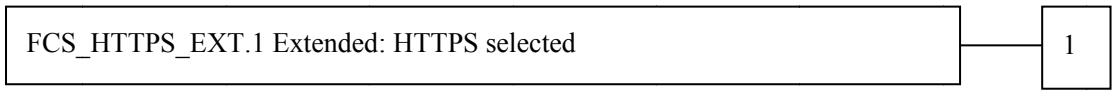
5.3 FCS_HTTPS_EXT Extended: HTTPS selected

Family behaviour:

Components in this family define 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 leveling:



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:

- 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:

- Failure of HTTPS session establishment

FCS_HTTPS_EXT.1 **Extended: HTTPS selected**

Hierarchical to: No other components

Dependencies: FCS_TLS_EXT.1 Extended: TLS 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 HTTPS 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.

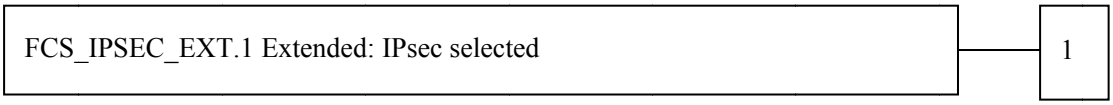
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4 FCS_IPSEC_EXT Extended: IPsec selected

Family behaviour:

This family addresses requirements for protecting communications using IPsec.

Component leveling:



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:

- 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:

- 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
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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-CBC-256 (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, using Main Mode for Phase 1 exchanges,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[selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23], 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 AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, 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

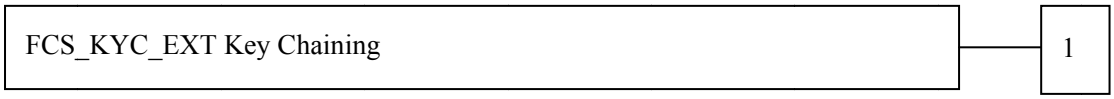
therefore placed in the FCS class with a single component.

5.5 FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family behaviour:

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 leveling:



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:

- 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:

- 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.

5.6 FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family behaviour:

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 leveling:

FCS_RBG_EXT.1 Extended: Random Bit Generation	1

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:

- 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:

- Failure of HTTPS session establishment

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 [selection: *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.

5.7 FCS_SMC_EXT Extended: Submask Combining

Family behaviour:

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 leveling:

FCS_SMC_EXT.1 Extended: Submask Combining	1

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:

- 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:

- 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) dependencies.

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.

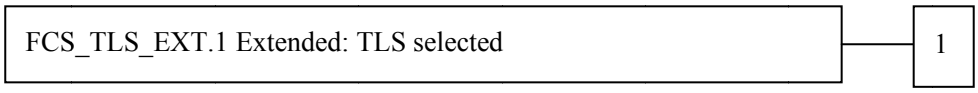
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.8 FCS_TLS_EXT Extended: TLS selected

Family behaviour:

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 leveling:



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:

- 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:

- Failure of TLS session establishment

FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to: No other components

Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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.

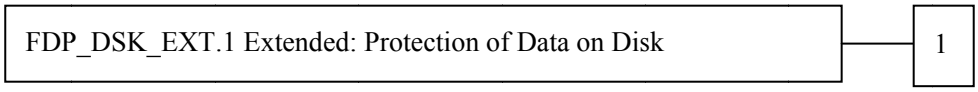
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.9 FDP_DSK_EXT Extended: Protection of Data on Disk

Family behaviour:

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

Component leveling:



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 Nonvolatile 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:

- 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:

- There are no auditable events foreseen.

FDP_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.

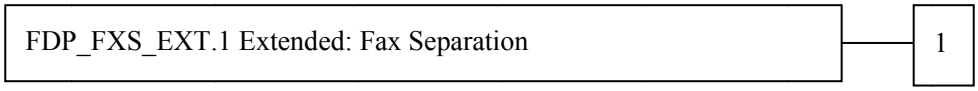
This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.10 FDP_FXS_EXT Extended: Fax Separation

Family behaviour:

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

Component leveling:



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:

- 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:

- There are no auditable events foreseen.

FDP_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.

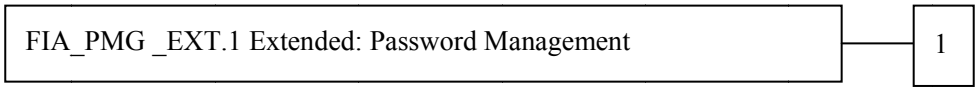
This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

5.11 FIA_PMG_EXT Extended: Password Management

Family behaviour:

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 leveling:



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:

- 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:

- 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 User passwords:

- 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*]];
- 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.

5.12 FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family behaviour:

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

Component leveling:

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	1

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:

- 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:

- 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.

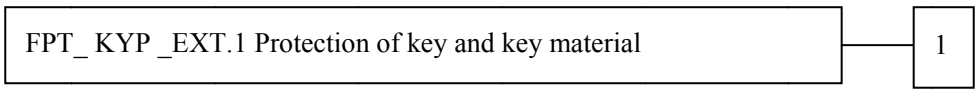
This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

5.13 FPT_KYP_EXT Extended: Protection of Key and Key Material

Family behaviour:

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

Component leveling:



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:

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

- 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:

- 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 nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.

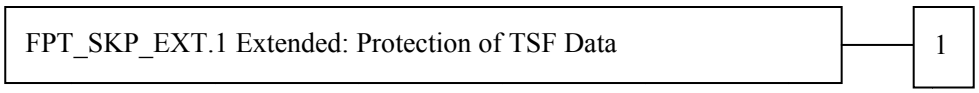
This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.14 FPT_SKP_EXT Extended: Protection of TSF Data

Family behaviour:

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 leveling:



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:

- 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:

- There are no auditable events foreseen.

FPT_SKP_EXT.1 Extended: Extended: Protection of TSF Data

Hierarchical to: No other components

Dependencies: No dependencies.

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.

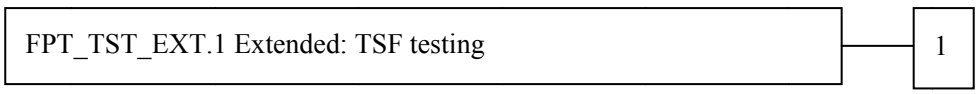
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.15 FPT_TST_EXT Extended: TSF testing

Family behaviour:

This family addresses the requirements for self-testing the TSF for selected correct operation.

Component leveling:



FPT_TST_EXT.1 TSF testing requires a suite of self-testing 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:

- 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:

- There are no auditable events foreseen.

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components

Dependencies: No dependencies.

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.

5.16 FPT_TUD_EXT Extended: Trusted Update

Family behaviour:

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

Component leveling:

FPT_TUD_EXT.1 Extended: Trusted Update	1

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:

- 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:

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),

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

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), 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 a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] 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.

6 SECURITY REQUIREMENTS

6.1 Notation

- **Bold typeface** indicates the portion of an SFR that has been "completed" or "refined" in HCD PP, relative to the original SFR definition in Common Criteria Part 2 or to its Extended Component Definition.
- *Italic typeface* indicates the text within an SFR that must be selected and/or completed in this ST.
- ***Bold italic typeface*** indicates the portion of an SFR that has been partially "completed" or "refined" in HCD PP and indicates the text within an SFR that must be selected and/or completed in this ST.
- [] indicates the portion indicating "Assignment" or "Selection". The result of "Assignment" or "Selection" in this ST is shown after the [] part is extracted after the text.
- A character in (), for example, an SFR component followed by (a) and (b), indicates that repetition was defined in HCD PP. To repeat further in ST, define as (a) (ssd).

6.2 Security functional requirements

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **All auditable events specified in Table 14,** [assignment: *other specifically defined auditable events*].

[assignment: *other specifically defined auditable events*].

- None

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 14**, [assignment: *other audit relevant information*].

[assignment: *other audit relevant information*]

- None

Table 14 - Auditable 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

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: ***an Administrator***] with the capability to read **all records** from the audit records.

[assignment: ***an Administrator***]
- U. ADMIN

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

Hierarchical to: No other components

Dependencies: FAU_SAR.1 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

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 Refinement: The TSF shall [selection, choose one of: *"prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

[selection, choose one of: *"prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

- "overwrite the oldest stored audit records"

[assignment: other actions to be taken in case of audit storage failure]

- None

FAU_STG_EXT.1 Extended: External Audit Trail Storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation,
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.1.

6.2.2 Class FCO: Communication

There are no class FCO requirements.

6.2.3 Class FCS: Cryptographic Support

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

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification),
FCS_COP.1(i) Cryptographic operation (Key Transport)]

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

- ***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" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")***
- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

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

[**selection:**

- ***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" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")***
- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

]

- 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" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")
- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes

[selection: P-521, no other curves]

- no other curves

FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b) 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 [selection: *128 bit, 256 bit*] that meet the following: No Standard.**

[selection: *128 bit, 256 bit*]

- 128 bit, 256 bit

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.

FCS_CKM.4 Cryptographic key 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.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection**:

For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].

For nonvolatile storage, the destruction shall be executed by a [selection: single, three or

more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;

] that meets the following: **[selection:** ***NIST SP800-88, no standard*****].**

[selection:

For volatile memory, the destruction shall be executed by [selection: ***powering off a device,*** **[assignment:** ***other mechanism that ensures keys are destroyed*****]].**

For nonvolatile storage, the destruction shall be executed by a [selection: ***single, three or more times*****] overwrite of key data storage location consisting of [selection:** ***a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern*****], followed by a [selection:** ***read-verify, none*****]. If read-verification of the overwritten data fails, the process shall be repeated again;**

]

- For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].
- For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;

[selection: ***powering off a device,*** **[assignment:** ***other mechanism that ensures keys are destroyed*****]]**

- powering off a device

[selection: ***single, three or more times*****]**

- single

[selection: ***a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern*****]**

- a static pattern

[selection: ***read-verify, none*****]**

- none

[selection: NIST SP800-88, no standard]

- no standard

FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

Hierarchical to: No other components.

Dependencies: **[**~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or~~
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

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

[assignment: one or more modes]
- CBC, GCM

[Selection: ***NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*****]**
- NIST SP 800-38A, NIST SP 800-38D

FCS_COP.1(b) (update) Cryptographic Operation (for signature generation/verification)

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation~~
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

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

that meets the following [**selection**:

Case: Digital Signature Algorithm
- ***FIPS PUB 186-4, "Digital Signature Standard"***

Case: RSA Digital Signature Algorithm
- ***FIPS PUB 186-4, "Digital Signature Standard"***

Case: Elliptic Curve Digital Signature Algorithm
- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

]

[selection:

- ***Digital Signature Algorithm (DSA) with key sizes (modulus) of*** **[assignment:** ***2048 bits***

***or greater*],**

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

  - RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater]

[assignment: *2048 bits or greater*]

- 2048 bits

[**selection**:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

]

- Case: RSA Digital Signature Algorithm
  - FIPS PUB 186-4, "Digital Signature Standard"

FCS_COP.1(b)(tls) Cryptographic Operation (for signature generation/verification)

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation~~
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

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

***bits or greater*]]**

that meets the following [**selection**:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

]

[selection:

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

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

[assignment: *2048 bits or greater*]

- 2048 bits

[assignment: *256 bits or greater*]

- 256 bits, 384bits

[**selection**:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

]

- Case: RSA Digital Signature Algorithm
  - FIPS PUB 186-4, "Digital Signature Standard"
- Case: Elliptic Curve Digital Signature Algorithm

- FIPS PUB 186-4, “Digital Signature Standard”
- The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).

[selection: P521, no other curves]

- no other curves

FCS_COP.1(b)(ipsec) Cryptographic Operation (for signature generation/verification)

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation~~
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

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

that meets the following [**selection**:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

]

[selection:

- ***Digital Signature Algorithm (DSA) with key sizes (modulus) of*** **[assignment:** ***2048 bits or greater*****],**
- ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of*** **[assignment:**

2048 bits or greater*], *or

- ***Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of* [assignment: *256 bits or greater*]]**

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

[assignment: *2048 bits or greater*]

- 2048 bits

[assignment: *256 bits or greater*]

- 256 bits, 384 bits

[**selection**:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***
- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

]

- Case: RSA Digital Signature Algorithm
  - FIPS PUB 186-4, "Digital Signature Standard"
- Case: Elliptic Curve Digital Signature Algorithm
  - FIPS PUB 186-4, "Digital Signature Standard"
  - The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").

[selection: P521, no other curves]

- no other curves

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

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_COP.1.1(c) Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [selection: ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: **[ISO/IEC 10118-3:2004**].

[selection: ***SHA-1, SHA-256, SHA-384, SHA-512***]

- SHA-1, SHA-256, SHA-384, SHA-512

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

Hierarchical to: No other components.

Dependencies: FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection: *CBC, GCM, XTS*] mode** and cryptographic key sizes **[selection: *128 bits, 256 bits*]** that meet the following: **AES as specified in ISO/IEC 18033-3, [selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619*]**.

[selection: *CBC, GCM, XTS*]

- XTS

[selection: *128 bits, 256 bits*]

- 256 bits

[selection: *CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619*]

- XTS as specified in IEEE 1619

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

Hierarchical to: No other components.

Dependencies: FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g) Refinement: The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC**-[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***], **key size** [assignment: **key size (in bits) used in HMAC**], **and message digest sizes [selection: *160, 224, 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."**

[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***]

- SHA-1, SHA-256, SHA-384

[assignment: **key size (in bits) used in HMAC**]

- 160, 256, 384 bits

[**selection: *160, 224, 256, 384, 512***]

- 160, 256, 384

FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 Extended: TLS 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 HTTPS using TLS as specified in FCS_TLS_EXT.1.

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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*].

[selection: *tunnel mode, transport 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-CBC-256 (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*].

[selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (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*]

- the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (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, using Main Mode for Phase 1 exchanges, 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, [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

[selection: *IKEv1, using Main Mode for Phase 1 exchanges, 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, [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]]

- IKEv1, using Main Mode for Phase 1 exchanges, 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*]

[selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*]

- RFC 4304 for extended sequence numbers

[selection: *no other RFCs for hash functions, RFC 4868 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 AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

[selection: *IKEv1, IKEv2*]

- IKEv1

[selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*]

- 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*]].

[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*]]

- 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*]

[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*]

- 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*].

[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*]

- 19 (256-bit Random ECP), 20 (384-bit Random ECP)

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.

[selection: *RSA, ECDSA*]

- RSA, ECDSA

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(f) Cryptographic operation (Key Encryption), FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1(i) Cryptographic operation (Key Transport)]

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEV or 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*].

[selection: *one, using a submask as the BEV or 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)*]]

- 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)*]

[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)*]

- key combining as specified in FCS_SMC_EXT.1

[selection: *128 bits, 256 bits*]

- 256 bits

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*]

- NIST SP 800-90A

[selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*]

- CTR_DRBG (AES)

FCS_RBG_EXT.1.2(network): The deterministic RBG shall be seeded by at least one 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.

[selection: [assignment: *number of software-based sources*] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)]

- [assignment: *number of hardware-based sources*] hardware-based noise source(s)

[assignment: *number of hardware-based sources*]

- 1

[selection: *128 bits, 256 bits*]

- 256 bits

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[selection: *ISO/IEC 18031:2011, NIST SP 800-90A*]

- NIST SP 800-90A

[selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*]

- Hash_DRBG (SHA-256)

FCS_RBG_EXT.1.2(ssd): The deterministic RBG shall be seeded by at least one 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.

[selection: [assignment: *number of software-based sources*] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)]

- [assignment: *number of hardware-based sources*] hardware-based noise source(s)

[assignment: *number of hardware-based sources*]

- 1

[selection: *128 bits, 256 bits*]

- 256 bits

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.

[selection: *exclusive OR (XOR), SHA-256, SHA-512*]

- SHA-256

FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to: No other components.

Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

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

].

[selection: *TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*]
- TLS 1.2 (RFC 5246)

[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

].

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
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

6.2.4 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based 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 15 and Table 16.**

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

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 15 and Table 16.**

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 15 and Table 16.***

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: ***rules that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*].

[assignment: ***rules that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*]

- None

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*]

- None

Table 15 - D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	***Operation:***	***Submit a document to be printed***	***View image or Release printed output***	***Modify stored document***	***Delete stored document***
	Job owner	(note 1) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Scan	***Operation:***	***Submit a document for scanning***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied

	Unauthenticated	denied	denied	denied	denied
Copy	***Operation:***	***Submit a document for copying***	***View scanned image or Release printed copy output***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	***Operation:***	***Submit a document to send as a fax***	***View scanned image***	***Modify stored image***	***Delete stored image***
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	denied	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	***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	(note 3) allowed	allowed	allowed	allowed
	U.ADMIN	(note 4) allowed	allowed	allowed	allowed
	U.NORMAL	(note 4) allowed	denied	denied	denied
	Unauthenticated	allowed	denied	denied	denied
Storage / retrieval	***Operation:***	***Store document***	***Retrieve stored document***	***Modify stored document***	***Delete stored document***
	Job owner	(note 1) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

Table 16 - D.USER.JOB Access Control SFP

		"Create" *	**"Read"**	**"Modify"**	**"Delete"**
Print	***Operation:***	***Create print job***	***View print queue / log***	***Modify print job***	***Cancel print job***
	Job owner	(note 1) allowed	allowed	allowed	allowed

	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Scan	***Operation:***	***Create scan job***	***View scan status / log***	***Modify scan job***	***Cancel scan job***
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	allowed	allowed	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	***Operation:***	***Create copy job***	***View copy status / log***	***Modify copy job***	***Cancel copy job***
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	***Operation:***	***Create fax send job***	***View fax job queue / log***	***Modify fax send job***	***Cancel fax send job***
	Job owner	(note 2) allowed	allowed	allowed	allowed
	U.ADMIN	allowed	allowed	allowed	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	***Operation:***	***Create fax receive job***	***View fax receive status / log***	***Modify fax receive job***	***Cancel fax receive job***
	Fax owner	(note 3) allowed	allowed	denied	denied
	U.ADMIN	(note 4) allowed	allowed	denied	allowed
	U.NORMAL	(note 4) allowed	allowed	denied	denied
	Unauthenticated	allowed	denied	denied	denied
Storage / retrieval	***Operation:***	***Create storage / retrieval job***	***View storage / retrieval log***	***Modify storage / retrieval job***	***Cancel storage / retrieval job***
	Job owner	(note 2) allowed	allowed	denied	allowed
	U.ADMIN	allowed	allowed	denied	allowed
	U.NORMAL	allowed	allowed	denied	denied
	Unauthenticated	denied	denied	denied	denied

Application notes:

The following Notes that are referenced in Table 15 and Table 16:

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.

FDP_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.

[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*]

- perform encryption in accordance with FCS_COP.1(d)

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

FDP_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.

6.2.5 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

[selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]]

- an administrator configurable positive integer within [assignment: range of acceptable values]

[assignment: *range of acceptable values*]

- positive integer within 1 to 10

[assignment: *list of authentication events*]

- Login attempts from the control panel or remote UIs or Printer Driver.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *list of actions*].

[selection: met, surpassed]

- met

[assignment: *list of actions*]

- lock out until preset time has passed that can set in 1 - 60 minutes

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]

- User Name, Role

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 User passwords:

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

[selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: *other characters*]]

- "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: other characters]

[assignment: *other characters*]

- "(space)", """, "'", "+", ",", "-", "/", ":", ";", "<", "=", ">", "?", "[", "¥", "]", "_", "`", "{", "|", "}", "~"

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 ")").

[selection: [assignment: *other supported lengths*], *no other lengths*]

- [assignment: *other supported lengths*]

[assignment: *other supported lengths*]

- Up to 24 characters

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*].

[selection: *SHA-1, SHA-256, SHA-512,* [assignment: *method of conditioning text string*]]

- SHA-1, SHA-256, [assignment: *method of conditioning text string*]

[assignment: *method of conditioning text string*]

- SHA-384

[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*]

- use no other pre-shared keys

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 Refinement: The TSF shall allow [assignment: *list of TSF mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is authenticated.

[assignment: *list of TSF mediated actions that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data*]

- Submit Fax receive job

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is

in progress.

[assignment: *list of feedback*]

- *, ●

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 Refinement: The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***]

- Submit Fax receive job

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

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

[assignment: list of user security attributes]

- User Name, 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: [assignment: *rules for the initial association of attributes*].

[assignment: rules for the initial association of attributes]

- None

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: [assignment: *rules for the changing of attributes*].

[assignment: *rules for the changing of attributes*]

- None

6.2.6 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

	FMT_SMF.1	Specification of Management Functions

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to **U.ADMIN.**

[selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

- disable, enable

[assignment: *list of functions*]

- TLS

FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.	
Dependencies:	FDP_ACC.1	Subset access control
	FMT_SMR.1	Security roles
	FMT_SMF.1	Specification of Management Functions

FMT_MSA.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

- query, modify, delete, [assignment: other operations]

[assignment: other operations]

- create

[assignment: *list of security attributes*]

- Refer to " Security attributes " in Table 17 - Management security attributes

[assignment: *the authorised identified roles*]

- Refer to " Authorised role(s)" in Table 17 - Management security attributes

Table 17 - Management of security attributes

Security attributes	Operation	Authorised role(s)
User Name	query	U.ADMIN, the owning U.NORMAL
	create,delete	U.ADMIN
Role	query	U.ADMIN
	create,modify,delete	U.ADMIN

FMT_MSA.3 Static attribute initialization

Hierarchical to:	No other components.	
Dependencies:	FMT_MSA.1	Management of security attributes
	FMT_SMR.1	Security roles

FMT_MSA.3.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to provide [selection,

choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- restrictive

FMT_MSA.3.2 Refinement: The TSF shall allow the [selection: ***U.ADMIN, no role***] to specify alternative initial values to override the default values when an object or information is created.

[selection: ***U.ADMIN, no role***]

- no role

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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 18.**

Table 18- Device management Function

Data	Operation	Authorised role(s)
User password	create, delete	**U.ADMIN**
	modify	**U.ADMIN, the owning U.NORMAL**
Audit log	query	**U.ADMIN**
Date/Time setting	modify	**U.ADMIN**
IPSec settings	query, modify	**U.ADMIN**
TLS settings	query, modify	**U.ADMIN**
Auto Reset Time setting	query, modify	**U.ADMIN**
Lockout policy settings	query, modify	**U.ADMIN**
Password policy settings	query, modify	**U.ADMIN**
Audit log export settings	query, modify	**U.ADMIN**
Firmware	modify	**U.ADMIN**

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [assignment:

list of management functions provided by the TSF].

[assignment: *list of management functions provided by the TSF*]

- Refer to Table 19.

Table 19– Management Functions

Management Functions
User Manegement Function
Date/Time setting Manegement Function
IPSec settings Manegement Function
TLS settings Manegement Function
Auto Reset Time setting Manegement Function
Lockout policy settings Manegement Function
Password policy settings Manegement Function
Audit log Manegement Function
Trusted Update Manegement Function

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

6.2.7 Class FPR: Privacy

There are no class FPR requirements.

6.2.8 Class FPT: Protection of the TSF

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 Refinement: The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

FPT_TUD_EXT.1 Extended: Trusted Update

Hierarchical to: No other components.

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),
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 a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] prior to installing those updates.

[selection: *published hash, no other functions*]

- no other functions

6.2.9 Class FRU: Resource Utilization

There are no class FRU requirements.

6.2.10 Class FTA: TOE Access

FTA_SSL.3 (LUI) TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 (LUI) The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: time interval of user inactivity]

- User inactivity at the control panel lasting for the specified period of time

FTA_SSL.3 (RUI) TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 (RUI) The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: time interval of user inactivity]

- User inactivity at the Remote UI lasting for the specified period of time

6.2.11 Class FTP: Trusted Paths/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_ITC.1.1 Refinement: The TSF shall **use [selection: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection: *authentication server, [assignment: other capabilities]*]** 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.**

[selection: *IPsec, SSH, TLS, TLS/HTTPS*]

- IPsec

[selection: *authentication server, [assignment: other capabilities]*]

- *[assignment: other capabilities]*

[assignment: other capabilities]

- File server, Audio log server, Time server

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

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for [assignment: ***list of services for which the TSF is able to initiate communications***].

[assignment: ***list of services for which the TSF is able to initiate communications***]

- Send service, Audit log service, Time service

FTP_TRP.1(a) Trusted path (for Administrators)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or

FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) Refinement: The TSF shall **use [selection, choose at least one of: IPsec, SSH, TLS, 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.**

[selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS]

- IPsec, TLS/HTTPS

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)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) Refinement: The TSF shall **use [selection, *choose at least one of: IPsec, SSH, TLS, 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**.

[selection, *choose at least one of: IPsec, SSH, TLS, TLS/HTTPS*]

- IPsec

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

[selection: ***the TSF, remote users***]

- remote users

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

6.3 Security Assurance Requirements

Table 20 lists the Security Assurance Requirements for Protection Profile for Hardcopy Devices, and related EAL1 augmented by ASE_SPD.1.

Table 20-TOE Security Assurance Requirements

Assurance class	Assurance components

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: 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
ATE: Tests	ATE_IND.1 Independent testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6.4 Security functional requirements rationale

6.4.1 The dependencies of security requirements

This section provides the justification for any dependencies not met

Table 21- The dependencies of security requirements

Functional Requirement	Dependencies required by CC	Dependencies satisfied by ST	Reason for not meeting dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1	N/A (dependencies are satisfied)
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	N/A (dependencies are satisfied)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	N/A (dependencies are satisfied)
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	N/A (dependencies are satisfied)
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	N/A (dependencies are satisfied)
FAU_STG.4	FAU_STG.1	FAU_STG.1	N/A (dependencies are satisfied)
FAU_STG_EXT.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1	N/A (dependencies are satisfied)
FCS_CKM.1(a)	FCS_COP.1(b) FCS_CKM_EXT.4	FCS_COP.1(b) FCS_CKM_EXT.4	N/A (dependencies are satisfied)
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)]	FCS_COP.1(a) FCS_COP.1(d) FCS_COP.1(g) FCS_CKM_EXT.4 FCS_RBG_EXT.1(network)	N/A (dependencies are satisfied)

Functional Requirement	Dependencies required by CC	Dependencies satisfied by ST	Reason for not meeting dependencies
	FCS_CKM_EXT.4 FCS_RBG_EXT.1	FCS_RBG_EXT.1(ssd)	
FCS_CKM_EXT.4	[FCS_CKM.1(a) or FCS_CKM.1(b)] FCS_CKM.4	FCS_CKM.1(a) FCS_CKM.1(b) FCS_CKM.4	N/A (dependencies are satisfied)
FCS_CKM.4	[FCS_CKM.1(a) or FCS_CKM.1(b)]	FCS_CKM.1(a) FCS_CKM.1(b)	N/A (dependencies are satisfied)
FCS_COP.1(a)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A (dependencies are satisfied)
FCS_COP.1(b)(update)	FCS_CKM.1(a) FCS_CKM_EXT.4	No dependencies	FCS_CKM.4 are not claimed because: Since only the verification is performed with the public key embedded in advance, generation and destruction of the encryption key are unnecessary.
FCS_COP.1(b)(tls)	FCS_CKM.1(a) FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	N/A (dependencies are satisfied)
FCS_COP.1(b)(ipsec)	FCS_CKM.1(a) FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	N/A (dependencies are satisfied)
FCS_COP.1(c)	No dependencies	No dependencies	N/A (no dependencies)
FCS_COP.1(d)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A (dependencies are satisfied)
FCS_COP.1(g)	FCS_CKM.1(b) FCS_CKM_EXT.4	FCS_CKM.1(b) FCS_CKM_EXT.4	N/A (dependencies are satisfied)
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	N/A (dependencies are satisfied)
FCS_IPSEC_EXT.1	FIA_PSK_EXT.1 FCS_CKM.1(a) FCS_COP.1(a) FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1	FIA_PSK_EXT.1 FCS_CKM.1(a) FCS_COP.1(a) FCS_COP.1(b) (ipsec) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1(network)	N/A (dependencies are satisfied)
FCS_KYC_EXT.1	[FCS_COP.1(e), or FCS_SMC_EXT.1, or FCS_COP.1(f), or FCS_KDF_EXT.1, and/or FCS_COP.1(i)]	FCS_SMC_EXT.1	N/A (dependencies are satisfied)
FCS_RBG_EXT.1 (network)	No dependencies	No dependencies	N/A (no dependencies)
FCS_RBG_EXT.1(ssd)	No dependencies	No dependencies	N/A (no dependencies)
FCS_SMC_EXT.1	FCS_COP.1(c)	FCS_COP.1(c)	N/A (dependencies are satisfied)
FCS_TLS_EXT.1	FCS_CKM.1(a)	FCS_CKM.1(a)	N/A (dependencies are

Functional Requirement	Dependencies required by CC	Dependencies satisfied by ST	Reason for not meeting dependencies
	FCS_COP.1(a) FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1	FCS_COP.1(a) FCS_COP.1(b)(tls) FCS_COP.1(c) FCS_COP.1(g) FCS_RBG_EXT.1(network)	satisfied)
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	N/A (dependencies are satisfied)
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	N/A (dependencies are satisfied)
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	N/A (dependencies are satisfied)
FDP_FXS_EXT.1	No dependencies	No dependencies	N/A (no dependencies)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	N/A (dependencies are satisfied)
FIA_ATD.1	No dependencies	No dependencies	N/A (no dependencies)
FIA_PMG_EXT.1	No dependencies	No dependencies	N/A (no dependencies)
FIA_PSK_EXT.1	FCS_RBG_EXT.1	No dependencies	FCS_RBG_EXT.1 is not claimed because: Not required because it is not selected in SFR.
FIA_UAU.1	FIA_UID.1	FIA_UID.1	N/A (dependencies are satisfied)
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	N/A (dependencies are satisfied)
FIA_UID.1	No dependencies	No dependencies	N/A (no dependencies)
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	N/A (dependencies are satisfied)
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	N/A (dependencies are satisfied)
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	N/A (dependencies are satisfied)
FMT_SMF.1	No dependencies	No dependencies	N/A (no dependencies)
FMT_SMR.1	FIA_UID.1	FIA_UID.1	N/A (dependencies are satisfied)
FPT_KYP_EXT.1	No dependencies	No dependencies	N/A (no dependencies)
FPT_SKP_EXT.1	No dependencies	No dependencies	N/A (no dependencies)
FPT_STM.1	No dependencies	No dependencies	N/A (no dependencies)
FPT_TST_EXT.1	No dependencies	No dependencies	N/A (no dependencies)
FPT_TUD_EXT.1	FCS_COP.1(b) FCS_COP.1(c)	FCS_COP.1(b) (update) FCS_COP.1(c)	N/A (dependencies are satisfied)

Functional Requirement	Dependencies required by CC	Dependencies satisfied by ST	Reason for not meeting dependencies
FTA_SSL.3(LUI)	No dependencies	No dependencies	N/A (no dependencies)
FTA_SSL.3(RUI)	No dependencies	No dependencies	N/A (no dependencies)
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1	N/A (dependencies are satisfied)
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1 FCS_TLS_EXT.1 FCS_HTTPS_EXT.1	N/A (dependencies are satisfied)
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1	N/A (dependencies are satisfied)

7 TOE Summary specification

7.1 User Authentication Function

- **Supported functional requirements: FIA_UAU.1, FIA_UID.1, FIA_UAU.7, FIA_ATD.1, FIA_USB.1, FIA_AFL.1, FTA_SSL.3(LUI), FTA_SSL.3(RUI)**

To identify and authenticate a legitimate user, the TOE requires identification and authentication of the user before the user operates the digital multifunction device in an operation panel or a remote UI. When a print job is input, identification authentication of a user requested through a printer driver on a client PC is performed. However, submission of a fax receiving job is permitted. [**FIA_UAU.1, FIA_UID.1**]

User authentication supports the following authentication methods:

- Internal Authentication

  Authentication is based on user information registered in the device.

For user authentication, the TOE prompts input of the user name, password, and the login destination. User authentication succeeds only if the user name and password matches the one at the specified destination. The password text area at the time of password input is displayed as "*" in the operation panel and "●" in the remote UI. [**FIA_UAU.7**]

The TOE maintains user names and roles as attributes for the user. If the user's identity is successfully authenticated, the attribute is allocated by issuing an access control token (ACT) for each user.[**FIA_ATD.1, FIA_USB.1**]

The TOE provides a lockout function in order to minimize invalid login attempts. [**FIA_AFL.1**]

Operation panel:	- Settings/Registration > Device Settings > Management Settings > User Management > Authentication Management > Use User Authentication > Register/Edit Authentication User
Remote UI:	- Settings/Registration > Management Settings > User Management > Authentication Management

The lockout function can be set only by U.ADMIN. The operation is as follows

Operation panel:	- Settings/Registration > Device Settings > Management Settings > Security Settings > Authentication/Password Settings > Authentication Function Settings>
Remote UI:	- Settings/Registration > Management Settings > Security Settings > Authentication/Password Settings > Authentication Function Settings>

The following conditions can be set for the lockout function. If the conditions are met, the account is locked out.

- Accumulate the number of failed login attempts from the operation panel/remote UI/printer driver, and lock out the account that failed to log in and deny login when the set number of allowable login attempts is reached. The allowable number of login attempts is set to 3 or less out of 1 - 10.
- The lockout time is set to 3 or grater out of 1 - 60. The user is not allowed to log in during the configured lockout time.

TOE has an automatic logout function that automatically logs out a logged-in user after a specified period of inactivity. The administrator can set the automatic logout time by setting the Auto Reset Time when logging

in from the operation panel or by session settings when logging in from the remote UI. **[FTA_SSL.3(LUI)] [FTA_SSL.3(RUI)]**

The automatic logout time settings can be set only by U.ADMIN. The operation is as follows

Operation panel:	- Settings/Registration > Device Settings > Preferences > Timer/Energy Settings > Auto Reset Time - Settings/Registration > Device Settings > Preferences> Timer/Energy Settings > Restrict Auto Reset Time
Remote UI:	- Settings/Registration > Preferences > Timer/Energy Settings > Power Save Settings > Auto Reset Time - Settings/Registration > Preferences > Timer/Energy Settings > Restrict Auto Reset Time

The following conditions can be set for the automatic logout function. If the conditions are met, the account is logged out.

- At the control panel, session timeout occurs after a specified period of user inactivity. A value from 10 seconds to 9 minutes can be specified (Initial value: 2 minutes).

The session settings can be set only by U.ADMIN. The operation is as follows

Remote UI:	- Settings/Registration > Preferences > Network Settings > Session Settings

The following conditions can be set for the session management function. If the conditions are met, the account is logged out.

- When the timeout period set by the session management setting function has elapsed without operating the Remote UI. Choose from 15 to 150 minutes (Initial value: 15 minutes).

7.2 Access Control Function

The TOE has the following access control functions for jobs and documents in jobs processed by the print function, scan function, copy function, fax function, and document storage and retrieval function of the TOE.

- print function: print process control function
- scanning function: scan process control function
- copy function: copy process control function
- fax function: Fax transmission process control function and fax reception process control function
- document store and retrieve function: document store and retrieve process control function

The TOE performs these access control functions by identifying the user name and identifying the role assigned to the user according to the contents of the ACT issued to the user who is identified and authenticated.

7.2.1 Print process control function

- **Supported functional requirements: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3**

TOE provides the following access control function for the print process. The user name assigned to print jobs is initialized with the name of the user that generated the job when the job is generated. No users can change the user name assigned to jobs.

When a print job is executed, TOE temporarily saves it without printing immediately. Furthermore, TOE determines the owner of a print job via the user name assigned to the print job, and performs the following access control.

[Submit a document to be printed, Create print job]

TOE allow all authenticated users (Job owner, U.ADMIN or U.NORMAL) to submit a document to be printed and to create print job. TOE does not allow Unauthenticated users.

The method for inputting print documents and creating print jobs is indicated below. The data for printing is held by the print function.

- The user executes printing via a printer driver from a client PC. User authentication is performed when a user uses the user authentication function of the printer driver to log in to the machine when printing. If user authentication is successful, the print job is sent with the user name assigned. The print job is not sent if user authentication fails.

[View image or Release printed output]

TOE allow Job owner (a user whom user name is same as use name of the print job) to view image or release printed output the images of digital documents for print jobs that are temporarily saved.

The method for viewing image or release printed output is indicated below.

- If a user logs in to the machine and selects <Print>, the list of data held for the logged in user is displayed.
- The print function can display images for the held data.
- The data held by the print function can be printed.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to view image or to release printed output.

[View print queue / log]

TOE allow Job owner or U.ADMIN to view print queue / log.

The method for viewing the print queue / log is indicated below.

- Job owner and U.ADMIN can log in to the control panel and use the <Status Monitor/Cancel> screen to check the list of jobs that are printing/waiting to be printed or check the job log. However, for Job owner, the job log only displays the jobs that the user owns (when the name of the user matches the user name of the print job). For jobs owned by other users, information such as job names and user names are masked and cannot be viewed in the print queue / log.
- If a Job owner logs in to the machine and selects <Print>, the list of data held for the logged in user is displayed.
- U.ADMIN can log in to the Remote UI and use the [Status Monitor/Cancel] screen to check the list of jobs that are printing/waiting to be printed or check the job log.

TOE does not allow U.NORMAL or Unauthenticated users to view print queue / log.

[Modify stored document, Modify print job]

TTOE allow Job owner to modify stored document and modify print job.

The method for modifying print document and modifying print job is indicated below.

- If a user logs in to the machine and selects <Print>, the list of data held for the logged in user is displayed. The image view function of the print function can be used to modify (delete) individual pages.
- If a user logs in to the machine and selects <Print>, the list of data held for the logged in user is displayed. If you select a job, you can change the job conditions (number of copies, print range, etc.)

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to Modify stored document and Modify print job.

[Delete stored document, Cancel print job]

TOE allow Job owner or U.ADMIN to delete stored document and cancel print job.

The method for deleting stored document and canceling print job is indicated below.

- If a Job owner logs in to the machine and accesses <Print>, the list of data held for the job owner is displayed. The job deletion function of the print function can be used to delete all print jobs and print documents.
- You can log in to the machine and select and cancel print jobs from the Status Monitor screen to delete print documents. Job owner can delete the print jobs they own and U.ADMIN can delete the print jobs and print documents of all users.
- U.ADMIN can log in to the Remote UI to delete the print jobs and print documents of all users from the [Status Monitor/Cancel] screen.

TOE does not allow U.NORMAL or Unauthenticated users to delete stored document and cancel print job.

7.2.2 Scan process control function

- **Supported functional requirements: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3**

TOE provides the following access control functions for the scan process. The user name assigned to scan jobs is initialized with the name of the user that generated the job when the scan job is generated. Also, no user can change the user name assigned to the scan document and the scan job.

Scan job has a function for temporarily saving scan jobs, which are [Delayed scan] and [Preview], respectively.

[Delayed scan]

When a scan job with the Delayed scan mode is executed, the machine temporarily saves the job without sending it until the specified time.

[Preview]

The TOE can be transmitted after the job contents are previewed and confirmed without transmitting immediately after reading the original when the scan job with the preview setting is inputted.

[Submit a document for scanning, Create scan job]

TOE allow Job owner, U.ADMIN or U.NORMAL to submit a document for scanning and create scan job.

The method for submitting a document for scanning and creating scan job is indicated below.

- Place the document on the scanner, log in to the operation panel, select <Scan and Send>, select the destination and press <START> button. The destination can be a file server. A scan job is generated, the document is read, and image data are stored. After that, it is transmitted to the file server from the LAN connected to the TOE.
- Place the document on the scanner, log in to the operation panel, select <Fax>, select the recipient and press <START> button. When the fax transmission document is previously set to be backed up, a scan job is generated, the document is read, and image data is stored. After that, it is transmitted to the specified file server from the LAN connected to the TOE.

TOE does not allow Unauthenticated users to submit a document for scanning and create scan job.

[View scanned image]

TOE allow Job owner to view scanned image.

The method for viewing scanned image is indicated below.

- Place the document on the scanner, log in to the operation panel, select <Scan and Send>, select the destination. Enable the <Preview> mode in the <Options> settings and press <START> button. The document is scanned and the scanned image is displayed on the touch panel display.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to view scanned image.

[View scan status / log]

TOE allow Job owner, U.ADMIN or U.NORMAL to view scan status / log.

The method for viewing scan status / log is indicated below.

- Log in to the operation panel and check the job status and job history by "Send" on the "Status Monitor". However, in the case of U.NORMAL, a job list containing another user's job can be displayed in the job status, but details such as the destination of another user's job are not displayed. Also, only log in user's job is displayed in the job history.
- U.ADMIN logs in to the remote UI, and the job status and job history can be checked by "Send" on the "Status Monitor/Cancel".

TOE does not allow Unauthenticated users to view scan status / log.

[Modify stored image]

TOE allow Job owner to modify stored image.

The method for modifying stored image is indicated below.

- Place the document on the scanner, log in to the operation panel, select <Scan and Send>, select the destination. Enable the <Preview> mode in the <Options> settings and press <START> button. The document is scanned and pages can be deleted or moved while the scanned image is displayed on the touch panel display.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to modify stored image.

[Modify scan job]

TOE allow Job owner or U.ADMIN to modify scan job.

The method for modifying scan job is indicated below.

- Select a job from the screen displayed by logging in to the machine and pressing <Status Monitor> <Send> <Job Status>. The destination can be changed by displaying <Details>.

TOE does not allow U.NORMAL or Unauthenticated users to modify scan job.

[Delete stored image, Cancel scan job]

TOE allow Job owner or U.ADMIN to delete stored image or cancel scan job.

The method for deleting stored image or canceling scan job is indicated below.

- Place the originals on the scanner, log in to the machine, select <Scan and Send>, select the destination, and press <START>. Press <Cancel> on the scanning screen to delete the scanned send image and delete the send job.
- Place the originals on the scanner, log in to the machine, select [Scan and Send], and select the destination. Then enable the <Preview> mode in <Options> and press <START>. Stop the send job with the send document displayed on the touch panel display after the originals are scanned to delete the send document and the send job.
- Place the originals on the scanner, log in to the machine, select <Scan and Send>, and select the destination. Then enable the <Delayed Send> mode in <Options> and press <START>. Display the send job status on the <Status Monitor> screen after the originals are scanned. Select a send job and press <Cancel> to delete the send document and send job. When the machine is set to back up sent fax documents, the scan document and scan job sent to the backup destination are deleted. However, a job owner can only delete send jobs when the name of the user matches the user name of the send job.
- U.ADMIN can log in to the Remote UI, select and cancel send jobs from the [Status Monitor/Cancel] screen to delete send documents and send jobs.

TOE does not allow U.NORMAL or Unauthenticated users to delete stored image or cancel scan job.

7.2.3 Copy process control function

- **Supported functional requirements: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3**

TOE provides the following access control function for the copy process. The user name assigned to copy

jobs is initialized with the name of the user that generated the job when the copy job is generated. No users can change the user name assigned to jobs.

[Submit a document for copying, Create copy job]

TOE allow Job owner, U.ADMIN or U.NORMAL to submit a document for copying or create copy job.

The method for submitting a document for copying or creating copy job is indicated below.

- Place the originals on the scanner, log in to the machine, and select <Copy>. Specify the required settings and press <START> button. A copy job is created and the originals are scanned.

TOE does not allow Unauthenticated users to submit a document for copying or create copy job.

[View scanned image or Release printed copy output]

TOE allow Job owner to view scanned image or release printed copy output.

The method for viewing scanned image or releasing printed copy output is indicated below.

- Place the originals on the scanner, log in to the machine, press <Copy>, and select <Merge Job Blocks> from <Options>. The image can be displayed by selecting a job that has been scanned by pressing <START> button and selecting <Display Image> from <Edit & Adjust>.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to view scanned image or release printed copy output.

[View copy status / log]

TOE allow Job owner or U.ADMIN to view copy status / log.

The method for view copy status / log is indicated below.

- You can check the job status and job log from the screen displayed by logging in to the machine and pressing <Status Monitor> > <Copy/Print>. However, for job owners, only their own jobs are displayed in the job log.
- U.ADMIN can check the job status and job log from the screen displayed by logging in to the Remote UI and clicking [Status Monitor/Cancel] > [Copy/Print].

TOE does not allow U.NORMAL or Unauthenticated users to view copy status / log.

[Modify stored image]

TOE allow Job owner to modify stored image.

The method for modifying stored image is indicated below.

- Place the originals on the scanner, log in to the machine, press <Copy>, and select <Merge Job Blocks> from <Options>. Press <START> and specify the page of a scanned job to delete that page.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to modify stored image.

[Modify copy job]

TOE does not have a function for modifying copy jobs.

Therefore, TOE does not allow job owner, U.ADMIN, U.NORMAL, or Unauthenticated users to modify copy jobs.

[Delete stored image, Cancel copy job]

TOE allow Job owner or U.ADMIN to delete stored image and cancel copy job.

The method for deleting stored image and canceling copy job is indicated below.

- Place the originals on the scanner, log in to the machine, select <Copy>, and press <START>. Job owners can press <Cancel> on the original scanning screen to cancel the copy job and delete the scanned image data.
- Place the originals on the scanner, log in to the machine, select <Copy>, and press <START>. The originals are scanned and copying is executed. Cancel a copy job that is executing on the Status Monitor screen to cancel the copy job and delete the scanned image data.
- U.ADNIN can log in to the Remote UI and select and cancel jobs from the [Status Monitor/Cancel] screen to cancel copy jobs and delete scanned image data.

TOE does not allow U.NORMAL or Unauthenticated users to delete stored image and cancel copy job.

7.2.4 Fax transmission process control

- **Supported functional requirements: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3**

TOE provides the following access control functions for the fax tarnsmission process. The user name assigned to fax send job is initialized with the name of the user that generated the job when the fax send job is generated. Also, no user can change the user name assigned to the fax send document and the fax send job.

Fax send job has a function for temporarily saving fax send jobs, which are [Delayed scan] and [Preview], respectively.

[Delayed scan]

When a fax send job with the Delayed scan mode is executed, TOE temporarily saves the job without sending it until the specified time.

[Preview]

TOE can be transmitted after the job contents are previewed and confirmed without transmitting immediately after reading the original when the fax send job with the preview setting is inputted.

[Submit a document to send as a fax, Create fax send job]

TOE allow Job owner, U.ADMIN or U.NORMAL to submit a document to send as a fax, create fax send

job.

The method for submitting a document for submitting a document to send as a fax, creating fax send job is indicated below.

- Place the document on the scanner, log in to the operation panel, select <Fax>, select the destination and press <START> button. A fax send job is generated, the document is read, and image data are stored. After that, it is faxed throuth the PSTN connected to the TOE.

TOE does not allow Unauthenticated users to submit a document to send as a fax, create fax send job.

[View scanned image]

TOE allow Job owner to view scanned image.

The method for viewing scanned image is indicated below.

- Place the document on the scanner, log in to the operation panel, select <Fax>, select the destination. Enable the <Preview> mode in the <Options> settings and press <START> button. The document is scanned and the scanned image is displayed on the touch panel display.

However, when faxing a received fax document in the Memory RX Inbox from the <Fax/I-Fax Inbox>, you cannot preview the fax send image.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to view scanned image.

[View fax job queue / log]

TOE allow Job owner, U.ADMIN or U.NORMAL to view fax job queue / log.

The method for viewingfax job queue / log is indicated below.

- Log in to the operation panel and check the job status and job history by "Send" on the "Status Monitor". However, in the case of U.NORMAL, a job list containing another user's job can be displayed in the job status, but details such as the destination of another user's job are not displayed. Also, only log in user's job is displayed in the job history.
- U.ADMIN logs in to the remote UI, and the job status and job history can be checked by "Send" on the "Status Monitor/Cancel".

TOE does not allow Unauthenticated users to view fax job queue / log.

[Modify stored image]

TOE allow Job owner to modify stored fax send image.

The method for modifying fax send image is indicated below.

- Place the document on the scanner, log in to the operation panel, select <Fax>, select the destination. Enable the <Preview> mode in the <Options> settings and press <START> button. The document is scanned and pages can be deleted or moved while the scanned image is displayed on the touch panel display.

However, when faxing a received fax document in the Memory RX Inbox from the <Fax/I-Fax Inbox>, you cannot modify stored fax send image.

TOE does not allow U,ADMIN, U.NORMAL or Unauthenticated users to modify fax send image.

[Modify fax send job]

TOE allow Job owner or U.ADMIN to modify fax send job.

The method for modifying fax send job is indicated below.

- Select a job from the screen displayed by logging in to the machine and pressing <Status Monitor> <Send> <Job Status>. The destination can be changed by displaying <Details>.

TOE does not allow U.NORMAL or Unauthenticated users to modify fax send job.

[Delete stored image, Cancel fax send job]

TOE allow Job owner or U.ADMIN to delete stored image or cancel fax send job.

The method for deleting stored image or canceling fax send job is indicated below.

- Place the originals on the scanner, log in to the machine, select <Fax>, select the destination, and press <START>. Press <Cancel> on the scanning screen to delete the scanned fax send image and delete the fax send job.
- Place the originals on the scanner, log in to the machine, select [Fax], and select the destination. Then enable the <Preview> mode in <Options> and press <START>. Stop the fax send job with the fax send image displayed on the touch panel display after the originals are scanned to delete the stored image and the fax send job.
- Place the originals on the scanner, log in to the machine, select <Fax>, and select the destination. Then enable the <Delayed Send> mode in <Options> and press <START>. Display the send job status on the <Status Monitor> screen after the originals are scanned. Select a fax send job and press <Cancel> to delete the stored image and fax send job. However, a job owner can only delete fax send jobs when the name of the user matches the user name of the fax send job.
- U.ADMIN can log in to the Remote UI, select and cancel send jobs from the [Status Monitor/Cancel] screen to delete stored image and fax send jobs.

TOE does not allow U.NORMAL or Unauthenticated users to delete stored image or cancel fax send job.

7.2.5 Fax reception process control

- **Supported functional requirements: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3**

TOE provides the following access control function for the fax reception process. Since fax reception is performed by the system, users are not set for received images or received jobs. Access to the Memory RX Inbox where received faxes are saved is controlled via access privileges to the <Fax/I-Fax Inbox> button. When printing a received fax job, the print job access privileges are initialized with the user name that operated the received job. User names assigned to documents and jobs cannot be changed by any user.

TOE does not immediately print digital documents of fax receive job and instead saves them to the Memory RX Inbox. Access to the inbox is limited to Fax owner (U. ADMIN Allows Access to Inbox U. NORMAL) and U.ADMIN, and provides the following access control.

[Receive a fax and store it, Create fax receive job]

When TOE receives a fax document sent from outside, it saves the received fax images to the Memory RX Inbox and creates a received fax job. Therefore, all users can be considered allowed to save received fax images and create fax receive job.

[View fax image or Release printed fax output]

TOE allow Fax owner and U.ADMIN to view fax image or release printed fax output.

The method for viewing received fax images is indicated below.

- Log in to the machine, press <Fax/I-Fax Inbox> <Memory RX Inbox>, and open <Memory RX Inbox>. A list of the held fax data is displayed. You can select data and select <Display Image> to display the received fax images.
- An U.ADMIN can also display images by logging in to the Remote UI, clicking [Access Received/Stored Files] [Memory RX Inbox] [Memory RX Inbox], and selecting held received fax data.

The method for releasing printed fax output is performed as indicated below, and the fax data is erased after printing.

- Log in to the machine, press <Fax/I-Fax Inbox> <Memory RX Inbox>, and open the Memory RX Inbox. A list of the held fax data is displayed. Select the data, and press <Print> to print the fax image.

TOE does not allow U.NORMAL (other than Faxowner) and Unauthenticated users to view fax image or release printed fax output.

[View fax receive log]

TOE allow Fax owner, U.ADMIN or U.NORMAL to view fax receive log.

The method for viewing fax receive log is indicated below.

- You can display the received fax job status by logging into the machine and displaying the <Job Status> screen in <Status Monitor> <Receive>. You can also switch to the <Job Log> screen to display the list of received faxes.
- U.Admin can also log in to the Remote UI and check [Job Status] and [Job Log] under [Receive] on the [Status Monitor/Cancel] screen.

TOE does not allow Unauthenticated users to View fax receive log.

[Modify image of received fax]

TOE allow Fax owner or U.ADMIN to Modify image of received fax.

The method for Modifying image of received fax is indicated below.

- Log in to the machine, press <Fax/I-Fax Inbox> <Memory RX Inbox>, and open <Memory RX Inbox>. A list of the held fax data is displayed. You can select data and select <Display Image> to display the received fax images. Pages can be deleted while the image data is displayed on the touch panel display.

TOE does not allow U.NORMAL (other than Faxowner) or Unauthenticated users to Modify image of received fax.

[Modify fax receive job]

TOE does not have a function for modifying fax receive job.

Therefore, TOE does not allow Fax owner, U,ADMIN, U.NORMAL, or unauthenticated users to modify fax receive job.

[Delete image of received fax]

TOE allow Fax owner or U.ADMIN to delete image of received fax.

The method for deleting image of received fax is indicated below.

- Log in to the machine, press <Fax/I-Fax Inbox> <Memory RX Inbox>, and open <Memory RX Inbox>. A list of the held fax jobs is displayed. Select the data and press <Delete> to delete the received fax image.
- An administrator can log in to the Remote UI, click [Access Received/Stored Files] [Memory RX Inbox] [Memory RX Inbox], select the held received fax job, and click [Delete] to delete the received fax image.

TOE does not allow U.NORMAL(other than Faxowner) or Unauthenticated users to delete image of received fax.

[Cancel fax receive job]

TOE allow U.ADMIN to cancel fax receive job.

The method for canceling fax receive job is indicated below.

- You can log in to the machine, press <Status Monitor> <Receive> <Job Status>, select the held fax receive job, and press <Cancel> to delete the fax receive job.
- You can also log in to the Remote UI, click [Status Monitor/Cancel] [Job Status] under [Receive] [Cancel] to delete the fax receive job.

TOE does not allow Fax owner, U.NORMAL or Unauthenticated users to cancel fax receive job.

7.2.6 Document store and retrieve process control function

- **Supported functional requirements: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3**

TOE provides the following access control function for the document store and retrieve process.The user

name assigned to document store and retrieve process jobs is initialized with the name of the user that generated the job when the document store and retrieve process job is generated. No users can change the user name assigned to jobs.

TOE has a function for saving digital documents scanned from a scanner to the Advanced Box (Advanced Space). The destination to store the documents is a personal space inside the Advanced Box (Advanced Space) that only the logged in user can access.

[Store document, Create retrieval job]

TOE allow Job owner, U.ADMIN or U.NORMAL to store document and create retrieval job.

The method for store document and create retrieval job is indicated below.

- For a store job, place the original on the scanner, log in to the control panel, press <Scan and Store> <Advanced Box> <Personal Space>, and select the personal space of the user. When the Start button is pressed, the store job is generated, the original is scanned, and an image data file is generated and stored in the personal space.

TOE does not allow Unauthenticated users to store document and create retrieval job.

[Retrieve stored document, Create retrieval job]

TOE allow Job owner or U.ADMIN to retrieve stored document and create retrieval job.

The method for retrieving stored document and creating retrieval job is indicated below.

- For a retrieve job, log in to the control panel, press <Access Stored Files> <Advanced Box> <Personal Space>, and select the stored file. You can press <Print> to create a print job for retrieving a document.
- In <Fax/I-Fax Inbox>, U.ADMIN can send received fax documents in the Memory RX Inbox to a file server in the TIFF or PDF file formats. They can also send them via a fax line.

TOE does not allow U.NORMAL or Unauthenticated users to retrieve stored document and create retrieval job.

[View storage / retrieval log]

TOE allow Job owner, U.ADMIN or U.NORMAL to view storage / retrieval log.

The method for viewing storage / retrieval log is indicated below.

- To display a store log, log in to the control panel, press <Store> <Job Log> on the <Status Monitor> screen.
- U.ADMIN can also log in to the Remote UI, click [Status Monitor/Cancel] [Job Log] under [Store], and select [Local Print] to display the job log for printing stored documents.
- To display a retrieve log, log in to the control panel, press <Status Monitor> <Copy/Print> <Job Log> <Local Print> or press <Send> <Job Log> on the <Status Monitor> screen.
- U.ADMIN can also log in to the Remote UI, click [Status Monitor/Cancel] [Job Log] under [Copy/Print], and select [Local Print] to display the retrieve log or click [Status Monitor/Cancel] [Job Log] under [Send] to display the retrieve log

TOE does not allow Unauthenticated users to view storage / retrieval log.

[Modify stored document]

TOE allow Job owner to modify stored document.

The method for modifying stored document is indicated below.

- Log in to the control panel, press <Access Stored Files> <Advanced Box> <Personal Space>, select the file, and press <Edit File> <Change File Name> to change the file name.

TOE does not allow U.ADMIN, U.NORMAL or Unauthenticated users to modify stored document.

[Modify storage / retrieval job]

TOE does not have a function for modifying storage / retrieval job.

Therefore, TOE does not allow Job owner, U.ADMIN or U.NORMAL or unauthenticated users to modify storage / retrieval job.

[Delete stored document]

TOE allow Job owner or U.ADMIN to delete stored document.

The method for deleting stored document is indicated below.

- The job owner can log in to the control panel, press <Access Stored Files> <Advanced Box> <Personal Space>, select the file, and press <Edit File> <Delete> to delete the store document.
- U.ADMIN can log in to the control panel and press <Settings/Registration> <Function Settings> <Store/Access Files> <Advanced Box Settings> <Delete All Personal Spaces> to delete the store document.
- U.ADMIN can log in to the Remote UI to delete saved documents in [Settings/Registration] [Store/Access Files] [Advanced Box Settings] [Delete Personal Space].

TOE does not allow U.NORMAL or Unauthenticated users to delete stored document.

[Cancel storage / retrieval job]

TOE allow Job owner or U.ADMIN to cancel storage / retrieval job.

The method for canceling storage / retrieval job is indicated below.

- The job owner can press <Cancel> or <STOP> displayed on the control panel after generating a store job to delete the store job. They can also press <Cancel> in <Job Status> for <Copy/Print> or <Store> on the <Status Monitor> screen to delete the store job.
- U.ADMIN can log in to the Remote UI, click [Status Monitor/Cancel] [Job Status] under [Store], and click the cancel button to delete the store job.
- A job owner or U.ADMIN select the received fax document in the Memory RX Inbox from the <Fax/I-Fax Inbox> and select the destination. Then enable the <Delayed Send> mode in <Options> and

press <START>. Display the send job status on the <Status Monitor> screen. To display a transmission job status of a status confirmation screen. Select a send job and press <Cancel> to delete the send document and send job. However, a job owner can only delete a scan job when the name of the user matches the user name of the send job.

TOE does not allow U.NORMAL and Unauthenticated users to cancel storage / retrieval job.

7.3 PSTN Fax-Network Separation Function

- **Supported functional requirements:FDP_FXS_EXT.1**

The TSF prohibits communication via the fax I/F except for transmission and reception of user data using the SuperG3 protocol and the G3 protocol. Thus, the PSTN is controlled so as not to be able to intrude into the network. **[FDP_FXS_EXT.1]**

The TOE fax I/F is used only for sending and receiving faxes, not for other purposes.

The following measures are taken against unauthorized fax jobs and communications using fax I/Fs. When sending or receiving a job using a fax I/F, first, negotiation of the SuperG3 protocol and the G3 protocol is performed with the opposite side, and if the negotiation is not successful, the line is disconnected. In this way, attempts to communicate with protocols other than the SuperG3 protocol and the G3 protocol are blocked to prevent unauthorized transmission and reception.
This function is always enabled and there is no interface to control the operation.

7.4 SSD Encryption Function

- **Supported functional requirements:FDP_DSK_EXT.1**

All access to the TOE embedded SSD is via an SSD encryption chip mounted on the TOE controller board. Thus, all data including user data and TSF data input/output between the controller board and the TOE built-in SSD are encrypted, and the encrypted data are stored in the TOE built-in SSD.
[FDP_DSK_EXT.1.1]

The SSD encryption function is automatically enabled when an SSD is connected to the TOE and started for the first time, and since there is no interface to control the operation, there is no need for U.ADMIN or the user to set anything for the SSD encryption function of the TOE. **[FDP_DSK_EXT.1.2]**

When data including user data and TSF data is written to the TOE built-in SSD, encryption is performed via the SSD encryption chip before writing to the TOE built-in SSD. Also, when reading from the TOE built-in SSD, all reading is performed through the SSD encryption chip. To secure confidentiality of all data including user data and TSF data stored in a TOE built-in SSD by an encryption/decryption function.

7.4.1 Encryption/Decryption Function

- **Supported functional requirements:FCS_COP.1(d)**

To ensure the confidentiality of user data and TSF data stored in the TOE built-in SSD from all interfaces, the TOE performs the following encryption operations to encrypt all data stored in the TOE built-in SSD.
[FCS_COP.1(d)]

- To encrypt data written to a TOE built-in SSD.
- To decrypt data read from a TOE built-in SSD.

The encryption algorithm and key used for encryption operation are as follows.

- AES as specified in ISO/IEC 18033-3
- XTS as specified in IEEE 1619
- Cryptographic key size: 256 bits

7.4.2 Cryptographic key management function

- **Supported functional requirements:FCS_CKM.1(b), FCS_CKM.4, FCS_CKM.1(c), FCS_CKM_EXT.4, FCS_RBG_EXT.1(ssd), FCS_KYC_EXT.1, FCS_SMC_EXT.1, FPT_KYP_EXT.1, FPT_SKP_EXT.1**

The CSP (Critical Security Parameter) handled by the SSD encryption function is explained.

CSP identification	Description	Storage	State	Method of destruction
cryptographic key	A key for encryption	RAM in the encryption chip	plaintext	Lost due to TOE power loss
key seed	The internal state V and C of the DRBG and the seed value used for AES encryption key generation.	FLASH memory in the encryption chip	plaintext	Overwrite once with fixed value (0xFF)

Next, the life cycle (How to generate, manage, and destroy) of the encryption key is described.

[How to Generate Cryptographic Keys]

The TOE generates a key seed to be used in the SSD encryption function based on the following specifications when an administrator instructs the destruction/regeneration of the key seed at the time of the first connection (That is, at the time of TOE production) or at the time of TOE disposal between the encryption chip and the TOE controller.

The encryption chip generates Entropy Input (640 bits) and Nonce (256 bits) input to the DRBG using an entropy generation function using a random number generator using a ring oscillator as one hardware-based noise source. Entropy Input, generated by the entropy generator, has a minimum entropy of 400 bits, and Nonce has a minimum entropy of 160 bits. By inputting these values into DRBG, internal states V and C of DRBG are initialized. Then, the DRBG internal states V and C are stored in the FLASH memory in the encryption chip as a key seed as a source of the encryption key. **[FCS_RBG_EXT.1(ssd)]**

The TOE inputs a key seed (DRBG internal state V, C) to the DRBG, discards the random number generated at the first time, and computes 2 cipher keys of 256 bits by performing submask coupling using SHA -256 with internal states V and C as submasks at the second and third random number generation. **[FCS_SMC_EXT.1, FCS_COP.1(c), FCS_CKM.1(b)]**

After that, TOE encrypts all data stored in the TOE built-in SSD.

When the power is turned on next time, the encryption chip automatically reconstructs the encryption key based on the key seed and stores it in the RAM.

[How to Manage Cryptographic Keys]

Entropy generation functions are used to supply sufficient entropy to the DRBG internal states V and C which are submasks. Since a cipher key of 256 bit length is constituted by performing submask combination (internal processing by Hash DRBG based on SP 800 -90 A) to this submask, the strength (256 bits) of the cipher key is maintained at each stage of the key chain. **[FCS_KYC_EXT.1]**

The TOE stores the key seed from which the encryption key originates in clear text in FLASH memory in the encryption chip. The encryption key is stored only on the RAM in the encryption chip and not in the FLASH memory.

Since the encryption chip is mounted on the TOE controller board and the FLASH memory in the encryption chip is not a Field-Replaceable Nonvolatile Storage Device, a portion of the key chain is not stored in a plaintext, Field-Replaceable Nonvolatile Storage Device. **[FPT_KYP_EXT.1]**

There is no TOE interface to read the key seed from FLASH memory in the encryption chip out of the encryption chip. Since there is no interface for reading the encryption key from the RAM in the encryption chip outside the encryption chip, the key seed and the encryption key are protected from exposure. **[FPT_SKP_EXT.1]**

[How to Destroy the Cryptographic Key]

The encryption key exists only on the RAM in the encryption chip. Since the encryption key becomes unnecessary when the power is turned off, it is lost when the power is turned off. **[FCS_CKM_EXT.4/FCS_CKM.4]**

The key seed becomes unnecessary when the administrator determines that the encryption key needs to be changed, such as when the TOE is discarded. The key seed is destroyed by an instruction from the operation panel. Destroy the key seed by overwriting it once with a fixed value (0xFF). **[FCS_CKM_EXT.4/FCS_CKM.4]**

7.5 LAN Data Protection Function

7.5.1 IPSec Encription Function

- **Supported functional requirements:FCS_COP.1(a), FCS_COP.1(c), FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b), FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FCS_COP.1(g)**

To ensure the confidentiality and integrity of user data and TSF data transmitted between the TOE and the file server/audit log server/time server, the TOE encrypts and decrypts all IP packets using IPSec as defined in RFC 4301 as follows. **[FTP_ITC.1, FCS_IPSEC_EXT.1.1]**

- Encrypting operation for IP packets sent to the LAN
- Decryption operation for IP packets received from the LAN

In order to ensure the confidentiality and integrity of user data and TSF data transmitted from the client PC to the TOE when a general user performs printing using the printer driver from the client PC, the TOE encrypts/decrypts all IP packets using IPSec specified in RFC 4301 as follows. [**FTP_TRP.1(b), FCS_IPSEC_EXT.1.1**]

- Encrypting operation for IP packets sent to the LAN
- Decryption operation for IP packets received from the LAN

In order to ensure the confidentiality and integrity of user data and TSF data sent and received from the client PC to the TOE, the TOE encrypts and decrypts all IP packets using IPSec specified in RFC 4301 as follows when an administrator performs page operation of the remote UI using a web browser from the client PC. For the protection of the remote UI operation, not only the IPSec encryption function but also the TLS encryption function described in 7.5.3may be used. [**FTP_TRP.1(a), FCS_IPSEC_EXT.1.1**]

- Encrypting operation for IP packets sent to the LAN
- Decryption operation for IP packets received from the LAN

The following cryptographic algorithms and keys are used to implement the IPSec protocol ESP as specified in RFC 4303. [**FCS_COP.1(a), FCS_COP.1(c)**]

Cryptographic algorithm	Cryptographic key sizes	List of Standards
AES-CBC+HMAC	128 bit, 256 bit	FIPS PUB 197(AES) NIST SP 800-38A(CBC) FIPS PUB198-1(HMAC)
AES-GCM	128 bit, 256 bit	FIPS PUB 197(AES) NIST SP800-38D(GCM)

- The Secure Hash Algorithm (SHA) used by the above HMAC is SHA-1. SHA-1 satisfies the Keyed-Hash Message Authentication Code specified in FIPS PUB 198-1 and the Secure Hash Standard specified in FIPS PUB 180-3. The message digest length is 160 bits. The key length used by HMAC is 160 bits. [**FCS_COP.1(g)**]

IPSec connection mode supports transport mode only. [**FCS_IPSEC_EXT.1.2**]

IPSec connection settings define multiple, prioritized rules as the Security Policy Database (SPD).

SPD defines the peer condition (IP address, port number) to which the rule applies, the method of communication with the peer (IKE and IPSec settings), and whether the rule itself is enabled or disabled.

When sending and receiving IP packets, it attempts to negotiate IKE from valid rules according to the SPD priority. If IKE is not established, the packet is dropped.

When IKE is established, the communication partner condition of the rule valid from the top of the SPD priority order is confirmed to be matched while maintaining the established IKE, and communication is performed by IPSec setting of the first matched rule. IP packets that do not meet the communication partner conditions of all SPDs are discarded.

If the communication cannot be performed by the first matching rule, the packet is discarded and the matching of the communication partner condition with the lower priority rule is not confirmed.
[FCS_IPSEC_EXT.1.3]

The specifications of the corresponding protocols in IPSec are as follows. [**FCS_IPSEC_EXT.1.4-7,9**]

- IKEv1 IKEv1 as defined in RFCs 2407, 2408, 2409, and 4109, RFC4304 for extended sequence numbers, and RFC4868 for hash functions
- IKEv1 payload cipher: AES-CBC-128/AES-CBC-256 as specified in RFC3602
- Payload ciphers fo IPSec ESP: AES-CBC-128/AES-CBC-256 specified in RFC 3602 and AES-GCM-128/AES-GCM-256 specified in RFC 4106
- IKEv1 Phase 1 Key Exchange Uses Main Mode Only (No Aggressive Mode)
- The supported DH groups are Group 14 (2048 bit), ECDH 256 bit, and ECDH 384 bit, and U.ADMIN sets which one to use. It is then determined by performing key exchange and key establishment during communication.

The SA lifetime of IKEv1 can be limited by specifying a time of no more than 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs. [**FCS_IPSEC_EXT.1.8**]

All IKE protocols perform peer authentication using either the RSA algorithm, the ECDSA algorithm, or a preshared key.[**FCS_IPSEC_EXT.1.10**]

IPSec preshared keys can be configured per SPD rule. [**FIA_PSK_EXT.1.1**]

The number of characters of the preshared key can be set from 22 to 24. Available characters can be any combination of uppercase or lowercase letters, numbers, or special characters ("!" , "@", "#", "$", "%", "^", "&", "*", "(", ")"). [**FIA_PSK_EXT.1.2**]

Only text-based preshared keys are used, subject to SHA-1, SHA-256, and SHA-384. As the hash algorithm used for the conditioning, one of SHA-1, SHA-256, and SHA-384 is selected and used by the negotiation of IKE phase 1.[**FIA_PSK_EXT.1.3**]

The settings of the IPsec encryption function are set from the management function from operation panel or the remote UI by U.ADMIN.

Operation panel:	- Settings/Registration > Device Settings > Preferences > Network > TCP/IP Settings > IPSec Settings
Remote UI:	- Settings/Registration > Preferences > Network Settings > IPSec Settings - Settings/Registration > Preferences > Network Settings > IPSec Policy List

7.5.2 IPSec Cryptographic key management Function

- **Supported functional requirements:FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM_EXT.4, FCS_CKM.4, FPT_SKP_EXT.1**

The CSP handled by the IPSec cryptographic key management function is described below.

CSP identification	Description	Storage	State	Method of destruction
preshared key	Shared key used for pre-shared key authentication in IKEv1	SSD	encripted	None
MFP key pair	Key pair of TOE used for authentication by digital signature method (RSA, ECDSA) in IKEv1	SSD	encripted	None
IKE cryptographic key	Cryptographic key for encryption used with IKEv1	RAM	plain text	Lost due to TOE power loss
DH key pair ECDH key pair	Public/private key generated during DH/ECDH key exchange	RAM	plain text	Lost due to TOE power loss
IPSec cryptographic key	Encryption key for cryptographic used with IPSec ESP	RAM	plain text	Lost due to TOE power loss
IPSec authentication key	Key for authentication used with IPSec ESP	RAM	plain text	Lost due to TOE power loss
DRBG internal state	DRBG internal state for generating random numbers	RAM	plain text	Lost due to TOE power loss

The life cycle of the CSP is described below.

[How to Generate Cryptographic Keys]

The TOE generates encryption keys for use with the IPSec encryption feature based on the following specifications:.

CSP identification	Cryptographic Algorithm/ Key Establishment Algorithm	List of Standards
MFP key pair	RSA(2048 bits)	NIST SP800-56B Rev1:6.3.1.1 rsakpg1-basic
	ECDSA(P-256, P-384)	FIPS PUB 186-4 NIST SP800-56A Rev3: 5.6.1.2.2
IKE cryptographic key	AES-CBC	FIPS PUB 197(AES) NIST SP800-38A(CBC)
DH key pair	DH(Group14)	NIST SP800-56A Rev3: 5.6.1.1 Approved Safe-Prime Groups
ECDH key pair	ECDH(P-256, P-384)	NIST SP800-56A Rev3: 5.7.1.2
IPSec cryptographic key	AES-CBC	FIPS PUB 197(AES) NIST SP800-38A(CBC)
	AES_GCM	FIPS PUB 197(AES) NIST SP800-38D(GCM)
IPSec authentication key	HMAC	FIPS PUB 198-1

The preshared key is set (registered/changed/deleted) by U.ADMIN using the management function of TOE from the operation panel or the remote UI. The pre-shared key text area is displayed as "*" in the operation panel and "●" in the remote UI. [**FPT_SKP_EXT.1**]

The IPSec authentication/DH/ECDH key pair is generated by negotiation during IPSec communication. For the MFP key pair, U.ADMIN can be generated using the management function of the TOE from the operation panel or the remote UI. [**FCS_CKM.1(a)**]

The TOE generates 128 bit or 256 bit AES-CBC encryption keys as IKE encryption keys using the 7.5.5 random number generation function when negotiating IPSec communications. The TOE generates an AES-CBC or AES-GCM encryption key with a key length of 128 or 256 bits using the 7.5.5 random number generation function when negotiating IPSec communications as an IPSec encryption key. [**FCS_CKM.1(b)**]

[Encryption key management method]

CSP identification	Management method
preshared key MFP key pair	It is encrypted by the SSD encryption function and stored in the TOE built-in SSD.
IKE cryptographic key / IPSec cryptographic key / IPSec authentication key / DH key pair / DRBG internal state	Store in RAM in plain text.

The pre-shared key, MFP key pair, IKE encryption key, IPSec encryption key, IPSec authentication key, DH key pair, and ECDH key pair are not read or browsed by using the management function of the TOE from the operation panel or the remote UI. [**FPT_SKP_EXT.1**]

[How to destroy the encryption key]

The pre-shared key and MFP key pair are encrypted and stored in the TOE built-in SSD. Therefore, it is not necessary to destroy it.

The IKE encryption key/IPSec encryption key/IPSec authentication key/DH key pair/ECDH key pair/DRBG internal state becomes unnecessary when the TOE is powered down after the IPSec communication ends, and is lost when the TOE is powered down. [**FCS_CKM_EXT.4/FCS_CKM.4**]

7.5.3 TLS Encription Function

- **Supported functional requirements:FCS_COP.1(a), FCS_COP.1(c), FCS_COP.1(g), FTP_TRP.1(a), FCS_TLS_EXT.1, FCS_HTTPS_EXT.1**

The TOE is encrypted/decrypted by TLS in order to ensure the confidentiality and integrity of user data and TSF data to be transmitted/received when U.ADMIN uses the TOE for the following purposes.

Perpose	User	Protocol
Management with the Remote UI using a Web Browser	U.ADMIN	TLS/HTTPS

TSF negotiates TLS communication between the TOE and the client PC when a connection request is made from a Web browser on the client PC to a Web page of the TOE by U.ADMIN, performs server authentication using the TLS protocol, establishes a session using TLS, and starts HTTPS communication (RFC 2818 compliant). **[FCS_HTTPS_EXT.1]**
However, IPSec encryption is always used for remote UI operations, and TLS encryption is not required for protection. [**FTP_TRP.1(a)**]

The encryption algorithm and key used for encryption operation are as follows. The AES encryption algorithm conforms to FIPS PUB 197. [**FCS_COP.1(a)**]

cryptographic algorithm	cryptographic key sizes	list of standards
AES-CBC	128 bit, 256 bit	NIST SP800-38A
AES-GCM	128 bit, 256 bit	NIST SP800-38D

TLS supports the following protocols. [**FCS_TLS_EXT.1**]

- TLS 1.2 (RFC 5246)

TLS supports the following ciphersuites. [**FCS_COP.1(a), FCS_COP.1(c), FCS_COP.1(g), FCS_TLS_EXT.1**]

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- 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

The settings of the TLS encryption function are set from the management function from operation panel or the remote UI by U.ADMIN.

Operation panel:	- Settings/Registration > Device Settings > Preferences > Network > TCP/IP Settings > TLS Settings
Remote UI:	- Settings/Registration > Preferences > Network Settings > TLS Settings

7.5.4 TLS Cryptographic key management Function

- **Supported functional requirements:FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4, FCS_CKM_EXT.4, FPT_SKP_EXT.1**

The CSP handled by the TLS cryptographic key management function is described below.

CSP identification	Description	Storage	State	Method of destruction
MFP key pair	Key pair of the TOE used for authentication with digital signature method (RSA or ECDSA).	SSD	encripted	None
ECDH key pair	Public/private key generated during ECDH	RAM	plain text	Lost due to TOE power loss
TLS premaster secret	Pre-master secret used for TLS communication	RAM	plain text	Lost due to TOE power loss
TLS session key	Cryptographic key for communication Encryption	RAM	plain text	Lost due to TOE power loss
DRBG internal state	DRBG internal state for generating random numbers	RAM	plain text	Lost due to TOE power loss

The life cycle of the CSP is described below.

[How to Generate Cryptographic Keys]

The TOE generates encryption keys for use with the TLS encryption feature based on the following specifications:.

CSP identification	Cryptographic Algorithm/ Key Establishment Algorithm	List of Standards
MFP key pair	RSA(2048 bits)	NIST SP800-56B Rev1:6.3.1.1 rsakpg1-basic
	ECDSA(P-256, P-384)	FIPS PUB 186-4

		NIST SP800-56A Rev3: 5.6.1.2.2
ECDH key pair	ECDH(P-256, P-384)	NIST SP800-56A Rev3: 5.7.1.2
TLS session key	AES-CBC(128 bits, 256 bits)	FIPS PUB 197(AES) NIST SP800-38A(CBC)
	AES-GCM(128 bits, 256 bits)	FIPS PUB 197(AES) NIST SP800-38D(GCM)

For the MFP key pair, U.ADMIN can be generated using the management function of the TOE from the operation panel or the remote UI. [**FCS_CKM.1(a)**]

The TOE generates a TLS session key/TLS pre-master secret/ECDH key pair using the 7.5.5 DRBG Function at the start of TLS communication.[**FCS_CKM.1(a), FCS_CKM.1(b)**]

[How to manage encryption keys]

CSP identification	**Cryptographic Algorithm/ Key Establishment Algorithm**
MFP key pair	Encrypt by SSD encryption function and store on TOE built-in SSD
TLS session key/TLS premaster secret /ECDH key pair/DRBG internal state	Store in plain text in RAM.

Even if the TOE management function is used from the operation panel or the remote UI, there is no function to read or browse the TLS session key/TLS pre-master secret/ECDH key pair or the MFP key pair stored in the TOE built-in SSD. [**FPT_SKP_EXT.1**]

[How to destroy the encryption key]

The MFP key pair is encrypted and stored on the TOE embedded SSD. Therefore, it is not necessary to destroy it.

The TLS session key/TLS pre-master secret/ECDH key pair/DRBG internal state is no longer needed when the TOE is powered down and is lost when the TOE is powered down. [**FCS_CKM_EXT.4/FCS_CKM.4**]

7.5.5 DRBG Function

- **Supported functional requirements:FCS_RBG_EXT.1(network), FCS_COP.1(c)**

The TOE performs random number generation based on the following specifications. The random numbers generated by the random number generation function are used by the IPSec encryption function and the TLS encryption function.

DRBG algolithm	**List of Standards**
CTR_DRBG(AES)	NIST SP800-90A

TOE performs random number generation by inputting an entropy sequence to CTR_DRBG according to NIST SP 800-90A. [**FCS_RBG_EXT.1.1(network)**]

As a noise source, a hardware random number generator built in the processor of TOE (Intel Atom processor E3930) is used as a noise source by 1 hardware base. When the RDSEED instruction is executed, a 32 bit bit string is extracted from the hardware random number generator.

When the TOE is started, the RDSEED instruction is executed 128 times, and the acquired 4096 bit bit string is input to the Linux PRNG, which is the entropy source. It is known from [Rambus 2012] that a bit string output from a hardware random number generator, which is a noise source, contains a minimum entropy of more than 0.5 bits per bit, and Linux PRNG contains entropy of at least 2048 bits.

When the TOE is requested to generate a random number, an entropy sequence having a minimum entropy of 384 bits is collected from the Linux PRNG, which is an entropy source, and input as a seed value into CTR_DRBG to generate a random number of 256 bits. [**FCS_RBG_EXT.1.2(network)**]

7.6 Signature Verification and Generation Function

7.6.1 TLS Signature Generation Function

- **Supported functional requirements:FCS_COP.1(b)(tls) , FCS_COP.1(c)**

When a TLS session is established, a signature is generated using the following algorithm based on FIPS PUB 186-4. [**FCS_COP.1(b)(tls)**]

- RSA Digital Signature Algorithm (rDSA) with key sizes of 2048 bits
- Elliptic Curve Digital Signature Algorithm (ECDSA) with key lengths of 256 and 384 bits

SHA-256, SHA-384, SHA-512 are used for signature generation. [**FCS_COP.1(c)**]

Here are the possible signature algorithms and hash combinations.

- RSA2048:SHA-256, RSA2048:SHA-384, RSA2048:SHA-512
- ECDSA-256:SHA-256
- ECDSA-384:SHA-384

7.6.2 IPSec Signature Verification/Generation Function

- **Supported functional requirements:FCS_COP.1(b)(ipsec), FCS_COP.1(c)**

In the authentication using the certificate in IKEv1 of IPSec, signature verification/generation is performed by the following algorithm based on FIPS PUB 186-4. [**FCS_COP.1(b)(ipsec)**]

- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of 2048 bits
- Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of 256 bits or 384 bits

A hash value calculated by SHA-256 or SHA-384 is used for signature verification/generation. [**FCS_COP.1(c)**]

Here are the possible signature algorithms and hash combinations.

- RSA2048:SHA-256, RSA2048:SHA-384
- ECDSA-256:SHA-256

- ECDSA-384:SHA-384

7.7 Self-Testing Function

- **Supported functional requirements:FPT_TST_EXT.1, FCS_COP.1(b)(update), FCS_COP.1(c)**

The TOE performs the following self-tests at start-up. [**FPT_TST_EXT.1**]

If an error is detected in the following self-test, the TOE displays an error code on the operation panel and stops starting the TOE.

Firmware Integrity Check

- The firmware is previously signed using RSA (key length 2048 bits) and SHA-256 based on FIPS PUB 186-4, and the integrity is verified by comparing a hash value obtained by decrypting the signature using a public key held in advance with a hash value calculated from the firmware itself. [**FCS_COP.1(b)(update), FCS_COP.1(c)**]

7.8 Audit Log Function

- **Supported functional requirements:FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FAU_STG_EXT.1, FMT_MTD.1**

The TOE generates an audit log when the following events occur. [**FAU_GEN.1]**

The items in the audit log are as follows. [**FAU_GEN.2]**

- Date and time of the event, subject identity, type of event, and the outcome (success or failure) of the event

the following items are also added for the following events.

- job completion: Type of job
- Unsuccessful User authentication/ identification: the user name of the authentication attempt
- Failure to establish session: Reason for failure

Auditable event	Details and Interfaces
Start-up of the audit functions	TOE power ON (Main Unit Power Switch, Operation Panel, Remote UI)
Shutdown of the audit functions	TOE power OFF (Main Unit Power Switch, Operation Panel, Remote UI)
Job completion	End of Print Job End of Scan Job End of Copy Job End of the fax transmission job End of the fax reception job End of the document store and retrieve Job *All of the above are interfaces related to FDP_ ACC.1/FDP_ACF.1

Unsuccessful User authentication/ identification	Attempting to log in from the operation panel Attempting to log in from the remote UI Authentication attempts from the printer driver
Use of Device management functions	Interface Usage Related to FMT_SMF.1
Use of User management functions	Interface Usage Related to FMT_SMF.1
Modification to the group of Users that are part of a role	Interface usage related to role registration/modification/deletion
Changes to the time	Interface usage related to the ability to manage date/time settings
Failure to establish session	IPSec session establishment failure for network communication Failure to establish TLS session for network communication

The date and time information recorded in the audit log is provided by the TOE. The date and time information of the TOE is set manually by using the following management function or by acquiring an accurate date and time from a time server and synchronizing the time. The time server is built in the user's office environment, and communication between the TOE and the time server is performed for all IP packets by encryption/decryption using IPSec by the LAN data protection function. In addition, the setting for using the time server for the time management of the TOE can be set only by the U.ADMIN from the operation panel or the remote UI. **[FPT_STM.1]**

Operation panel:	- Settings/Registration > Device Settings > Preferences > Timer/Energy Settings > Date/Time Settings - Settings/Registration > Device Settings > Preferences > Network > TCP/IP Settings > SNTP Settings
Remote UI:	- Settings/Registration > Preferences > Timer/Energy Settings > Date/Time Settings - Settings/Registration > Preferences > Network Settings > SNTP Settings

The TOE provides the following functions for exporting audit logs to the audit log server.

Only U.ADMIN can set the setting of the audit log exporting function from the remote UI through the management function.

Remote UI:	- Settings/Registration > Management Settings > Device Management > Export/Clear Audit Log > Settings for Auto Export Audit Logs

The audit log is exported to the audit log server as a csv file using the SMB protocol. The audit log is exported at the specified time, but when the audit log reaches 95% of the storage capacity (40,000 items), it is sent to the audit log server regardless of the specified time. If the transmission succeeds, the exported audit log is automatically deleted. If transmission fails, retry is performed multiple times. If it still fails, it is exported at the next specified time. All communication between the TOE and the audit log server is encrypted/decrypted by the IPSec encryption function. **[FAU_STG_EXT.1]**

TOE provides the following as an internal audit log storage function.

The administrator can view the audit log by exporting it as a CSV file from the following operations in the remote UI. This feature is only available to U.ADMIN. [**FAU_SAR.1**][**FAU_SAR.2**] [**FMT_MTD.1**]

Remote UI:	- Settings/Registration > Management Settings > Device Management > Export/Clear Audit Log > Export Audit Logs

The internal audit log data is stored in the TOE built-in SSD, and the confidentiality is protected by the SSD encryption function. This TOE has no function or interface to modify the contents of the audit log. Audit logs cannot be manually deleted because the automatic export feature is enabled. [**FAU_STG.1**]

Up to 40,000 audit logs are maintained. When the maximum number of audit logs to record is reached, the oldest stored audit log is deleted and a new audit log is saved. [**FAU_STG.4**]

7.9 Trusted Update Function

- **Supported functional requirements:FPT_TUD_EXT.1, FCS_COP.1(b)(update), FCS_COP.1(c)**

[Checking the Firmware Version]

The TSF shall provide U.ADMIN the ability to query the current version of the TOE firmware/software. U.ADMIN can check the current version of the firmware from the Remote UI and the operation panel by the following operations. [**FPT_TUD_EXT.1.1**]

Operation panel:	- Counter/Device Information Key > Device Info./Other > Check Device Configuration
Remote UI:	- Status Monitor/Cancel > Device Information

[Ability to Initiate Updates]

The TSF shall provide U.ADMIN the ability to initiate updates to TOE firmware/software. U.ADMIN can manually update the firmware by specifying the firmware to be updated by the following operations in the remote UI. [**FPT_TUD_EXT.1.2**]

Remote UI:	- Settings/Registration > Management Settings > License/Other > Register/Update Software > Manual Update

[Verify Firmware Updates]

The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism (Signature Verification by RSA Digital Signature Algorithm (rDSA) with key sizes of 2048 bits based on FIPS PUB 186-4 and SHA-256) prior to installing those updates. If firmware validation fails, the remote UI displays an error message and the update aborts. The firmware remains in the state it was in before the update started. [**FPT_TUD_EXT.1.3, FCS_COP.1(b)(update), FCS_COP.1(c)**]

7.10 Management Function

7.10.1 User Management Function

- **Supported functional requirements:FIA_PMG_EXT.1 , FMT_MTD.1, FMT_MSA.1, FMT_SMR.1, FMT_SMF.1**

The TOE limits operations on the following security attributes to the respective authorized roles. The following operations can be performed from the remote UI or the operation panel. [**FMT_MSA.1, FMT_SMF.1**]

Operation panel:	- The user name is displayed in the upper right of the operation panel after login. - Settings/Registration > Device Settings > Management Settings > User Management > Authentication Management > Register/Edit Authentication User (U.ADMIN Only)
Remote UI:	- Settings/Registration > Management Settings > User Management > Authentication Management (U.ADMIN Only)

The TOE limits operations on the following data to the respective authorized roles. The following operations can be performed from the remote UI or the operation panel. [**FMT_MTD.1, FMT_SMF.1**]

Operation panel:	- Settings/Registration > Device Settings > Management Settings > User Management > Authentication Management > Change Password (the owning U.NORMAL) - Settings/Registration > Device Settings > Management Settings > User Management > Authentication Management > Register/Edit Authentication User(U.ADMIN Only)
Remote UI:	- Settings/Registration > Management Settings > User Management > Authentication Management (U.ADMIN Only)

Data	**Operation**	**Authorised role(s)**
User password	modify	**the owning U.NORMAL**
	create,modify,delete	**U.ADMIN**

[User Password]

User passwords can contain uppercase, lowercase, numeric, and special characters ("!" , "@" , "#" , "$" , "%" , "^" , "&" , "*" , "(" , ")" , "(space)" , """ , "'" , "+" , "," , "-" , "/" , ":" , ";" , "<" , "=" , ">" , "?", "[", "¥", "]", "_", "`", "{", "|", "}", "~"). The minimum number of characters can be set to 15 or more by U.ADMIN. [**FIA_PMG_EXT.1**]

[Roles]

There are five types of roles called base roles: "Administrator", "Power User", "General User", "Limited User", and "Guest User". "Administrator" is an administrator base role, and other base roles are consumer roles.

If you want to create a new Custom Role , you can duplicate and edit from four types of Base Roles except "Guest User". However, custom roles based on the "Administrator" role and the "DeviceAdmin" and "NetworkAdmin" roles that have been registered as custom roles (administrators) beforehandare not used because they allow some administrative privileges.

In this configuration, the following two types of roles (U. ADMIN, U. NORMAL) are used. The TOE associates these roles with legitimate users and maintains them during remote UI and operations panel logins. [**FMT_SMR.1**]

- U.ADMIN
  Role with administrative privileges. Use the "Administrator" role.
- U.NORMAL
  A role for which you do not have administrative privileges. Use a custom role created from a base role "General User".

7.10.2 Device Management Function

- **Supported functional requirements:FMT_MTD.1, FMT_SMF.1, FMT_MOF.1, FIA_PMG_EXT.1**

The TOE can perform the following management functions to enable the security functions to function effectively. You can do this from the Remote UI or from the operation panel Settings/Registration > Device Settings. [**FMT_SMF.1**]

Also, the ability to enable or desable the security function [TLS encryption function] is limited to U.ADMIN. [**FMT_MOF.1**]

Management Function	Item	Description
Date/Time setting Manegement Function	Overview	Date and time information can be set. You can also set it to sync with the time server.
	Procedures	Operation panel: Settings/Registration > Device Settings > Preferences > Timer/Energy Settings > Date/Time Settings Operation panel: Settings/Registration > Device Settings > Preferences > Network > TCP/IP Settings > SNTP Settings Remote UI: Settings/Registration > Preferences > Timer/Energy Settings > Date/Time Settings Remote UI: Settings/Registration > Preferences > Network Settings > SNTP Settings
IPSec settings Manegement Function	Overview	Manage the Security Policy Database (SPD) that defines IPSec connections. The SPD defines the other party's conditions to which the conditions are applied, the negotiation and encryption methods, and whether the settings are enabled or disabled. The IKE configuration in the SPD allows pre-shared key enrollment and certificate selection as authentication methods. In the authentication/encryption algorithm setting, SHA1 and SHA2 (SHA 256, SHA 384) can be selected as the authentication hash, AES-CBC can be set as the encryption method, and the DH group can be selected. You can also configure the lifetime of IKE SAs.

		In the IPSec communication configuration in the SPD, ESP (SHA1, AES-CBC) can be specified as the IPSec SA lifetime specification and the authentication/encryption algorithm specification.
	Procedures	Operation panel: Settings/Registration > Device Settings > Preferences > Network > TCP/IP Settings > IPSec Settings Remote UI: Settings/Registration > Preferences > Network Settings > IPSec Settings Remote UI: Settings/Registration > Preferences > Network Settings > IPSec Policy List
TLS settings Manegement Function	Overview	The TLS cipher feature is defined to start or stop working. It is also possible to select an encryption key and a certificate to be used for TLS encryption communication. This selection determines the digital signature algorithm and key length to use when establishing a TLS session.
	Procedures	Operation panel: Settings/Registration > Device Settings > Management Settings > License/Other > Remote UI Operation panel: Settings/Registration > Device Settings > Preferences > Network > TCP/IP Settings > TLS Settings Remote UI: Settings/Registration > Management Settings > License/Other > Remote UI Remote UI: Settings/Registration > Preferences > Network Settings > TLS Settings
Auto Reset Time setting Manegement Function	Overview	The administrator can set the respective automatic logout times according to the Auto Reset time when logging in from the operation panel and the session setting when logging in from the remote UI. - Auto Reset Time: 10 seconds to 9 minutes (default 2 minutes) - Session settings: 15 to 150 minutes (default 15 minutes)
	Procedures	Operation panel: Settings/Registration > Device Settings > Preferences > Timer/Energy Settings > Auto Reset Time Operation panel: Settings/Registration > Device Settings > Preferences > Timer/Energy Settings > Restrict Auto Reset Time Remote UI: Settings/Registration > Preferences > Timer/Energy Settings > Power Save Settings > Auto Reset Time Remote UI: Settings/Registration > Preferences > Timer/Energy Settings > Power Save Settings > Restrict Auto Reset Time Remote UI: Settings/Registration > Preferences > Timer/Energy Settings > Network Settings
Lockout policy settings Manegement Function	Overview	The lockout tolerance and lockout time can be set. - Lockout tolerance: 1 to 10 (The default setting is 3 times or less.) - Lockout time: 1 to 60 minutes (The default setting is 3 minutes or more.)
	Procedures	Operation panel: Settings/Registration > Device Settings > Management Settings > Security Settings > Authentication/Password Settings > Authentication Function Settings Remote UI: Settings/Registration > Management Settings > Security Settings > Authentication/Password Settings >

		Authentication Function Settings
Password policy settings Manegement Function	Overview	To require the user to set a robust password, the following functions are provided to ensure the quality of the password. - Ability to set a minimum password length of 15 to 32 characters - Available Characters uppercase, lowercase, numeric, and special characters ("!" , "@" , "#" , "$" , "%" , "^" , "&" , "*" , "(" , ")" , "(space)" , """ , "'" , "+" , "," , "-" , "/" , ":" , ";" , "<" , "=" , ">" , "?", "[", "¥", "]", "_", "`", "{", "|", "}", "~").
	Procedures	Operation panel: Settings/Registration > Device Settings > Management Settings > Security Settings > Authentication/Password Settings > Password Settings Remote UI: Settings/Registration > Management Settings > Security Settings > Authentication/Password Settings > Password Settings
Audit log Manegement Function	Overview	Can retrieve internally stored audit logs You can configure the destination settings for sending audit logs to the audit log server.
	Procedures	Remote UI: Settings/Registration > Management Settings > Device Management > Export/Clear Audit Log
Trusted Update Manegement Function	Overview	Specify the firmware to update
	Procedures	Remote UI: Settings/Registration > Management Settings > License/Other > Register/Update Software > Manual Update

8 References

[Rambus 2012]
Analysis of Intel's Ivy Bridge Digital Random Number Generator, Cryptography Research a division of Rambus, 2012.

https://www.rambus.com/intel-ivy-bridge-random-number-generator/

Fin