



Xerox VersaLink C505
Color Multifunction Printer
Diskless model
Security Target

Version 1.1.8

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

August 2018

- Table of Contents -

| | | |
|--------|--|----|
| 1. | ST INTRODUCTION | 1 |
| 1.1. | ST Reference | 1 |
| 1.2. | TOE Reference | 1 |
| 1.3. | TOE Overview | 2 |
| 1.3.1. | TOE Type and Major Security Features..... | 2 |
| 1.3.2. | Environment Assumptions | 4 |
| 1.3.3. | Required Non-TOE Hardware and Software..... | 5 |
| 1.4. | TOE Description | 7 |
| 1.4.1. | User Assumptions | 7 |
| 1.4.2. | Logical Scope and Boundary | 7 |
| 1.4.3. | Physical Scope and Boundary..... | 13 |
| 1.4.4. | Guidance | 14 |
| 2. | CONFORMANCE CLAIMS | 15 |
| 2.1. | CC Conformance Claims | 15 |
| 2.2. | PP Claims, Package Claims | 15 |
| 2.2.1. | PP Claims..... | 15 |
| 2.2.2. | Package Claims..... | 15 |
| 2.2.3. | Conformance Rationale | 15 |
| 3. | SECURITY PROBLEM DEFINITION | 16 |
| 3.1. | Threats..... | 16 |
| 3.1.1. | Assets Protected by TOE..... | 16 |
| 3.1.2. | Threats..... | 18 |
| 3.2. | Organizational Security Policies | 19 |
| 3.3. | Assumptions | 19 |
| 4. | SECURITY OBJECTIVES | 20 |
| 4.1. | Security Objectives for the TOE | 20 |
| 4.2. | Security Objectives for the Environment..... | 21 |
| 4.3. | Security Objectives Rationale | 21 |
| 5. | EXTENDED COMPONENTS DEFINITION | 25 |
| 5.1. | Extended Components..... | 25 |

| | | |
|--------|--|----|
| 6. | SECURITY REQUIREMENTS..... | 26 |
| 6.1. | Security Functional Requirements | 30 |
| 6.1.1. | Class FAU: Security audit..... | 30 |
| 6.1.2. | Class FCS: Cryptographic support..... | 34 |
| 6.1.3. | Class FDP: User data protection..... | 35 |
| 6.1.4. | Class FIA: Identification and authentication | 37 |
| 6.1.5. | Class FMT: Security management | 41 |
| 6.1.6. | Class FPT: Protection of the TSF | 47 |
| 6.1.7. | Class FTP: Trusted path/channels | 48 |
| 6.2. | Security Assurance Requirements | 49 |
| 6.3. | Security Requirement Rationale | 50 |
| 6.3.1. | Security Functional Requirements Rationale | 50 |
| 6.3.2. | Dependencies of Security Functional Requirements | 54 |
| 6.3.3. | Security Assurance Requirements Rationale | 57 |
| 7. | TOE SUMMARY SPECIFICATION | 58 |
| 7.1. | Security Functions | 58 |
| 7.1.1. | Flash Memory Data Encryption (TSF_CIPHER) | 59 |
| 7.1.2. | User Authentication (TSF_USER_AUTH) | 59 |
| 7.1.3. | System Administrator's Security Management (TSF_FMT) | 62 |
| 7.1.4. | Customer Engineer Operation Restriction (TSF_CE_LIMIT) | 64 |
| 7.1.5. | Security Audit Log (TSF_FAU) | 64 |
| 7.1.6. | Internal Network Data Protection (TSF_NET_PROT) | 67 |
| 7.1.7. | Self Test (TSF_S_TEST)..... | 69 |
| 8. | ACRONYMS AND TERMINOLOGY | 70 |
| 8.1. | Acronyms | 70 |
| 8.2. | Terminology | 71 |
| 9. | REFERENCES | 74 |

- List of Figures and Tables –

| | |
|---|----|
| Figure 1: General Operational Environment | 5 |
| Figure 2: MFD Units and TOE Logical Scope | 8 |
| Figure 3: Authentication Flow for Store Print | 10 |
| Figure 4: MFD Units and TOE Physical Scope | 13 |
| Figure 5: Assets under and not under Protection | 17 |
| | |
| Table 1: Function Types and Functions provided by the TOE | 2 |
| Table 2: User Role Assumptions | 7 |
| Table 3: TOE Basic Functions | 8 |
| Table 4: Categories of TOE Setting Data | 17 |
| Table 5: Threats Addressed by the TOE | 18 |
| Table 6: Organizational Security Policy | 19 |
| Table 7: Assumptions | 19 |
| Table 8: Security Objectives for the TOE | 20 |
| Table 9: Security Objectives for the Environment | 21 |
| Table 10: Assumptions / Threats / Organizational Security Policies and the Corresponding Security Objectives | 22 |
| Table 11: Security Objectives Rationale for Security Problem | 22 |
| Table 12: Auditable Events of TOE and Individually Defined Auditable Events | 30 |
| Table 13: Operations between Subjects and Objects Covered by MFD Access Control SFP | 36 |
| Table 14: Rules for Access Control | 37 |
| Table 15: List of Security Functions | 41 |
| Table 16: Security Attributes and Authorized Roles | 42 |
| Table 17: Initialization property | 43 |
| Table 18: Operation of TSF Data | 43 |
| Table 19: Security Management Functions Provided by TSF | 45 |
| Table 20: Security Assurance Requirements | 49 |
| Table 21: Security Functional Requirements and the Corresponding Security Objectives | 50 |
| Table 22: Security Objectives to SFR Rationale | 51 |
| Table 23: Dependencies of Functional Security Requirements | 55 |
| Table 24: Security Functional Requirements and the Corresponding TOE Security Functions | 58 |
| Table 25: Management of security attributes | 61 |
| Table 26: Access Control | 62 |
| Table 27: Details of Security Audit Log Data | 64 |

1. ST INTRODUCTION

This chapter describes Security Target (ST) Reference, TOE Reference, TOE Overview, and TOE Description.

1.1. ST Reference

This section provides information needed to identify this ST.

| | |
|-------------------|--|
| ST Title: | Xerox VersaLink C505 Color Multifunction Printer Diskless model Security Target |
| ST Version: | V 1.1.8 |
| Publication Date: | August 6, 2018 |
| Author: | Fuji Xerox Co., Ltd. |

1.2. TOE Reference

This section provides information needed to identify this TOE.

The TOE is VersaLink C505S.

The TOE is identified by the following TOE name and ROM version.

| | | |
|------------------------|---|--------------|
| TOE Identification: | Xerox VersaLink C505 Color Multifunction Printer Diskless model | |
| Version: | Controller ROM | Ver. 1.12.32 |
| Manufacturer: | Fuji Xerox Co., Ltd. | |

NOTE: “Xerox VersaLink C505 Color Multifunction Printer Diskless model” refers to a configuration not equipped with a hard disk:

The followings are the target products.

Xerox VersaLink C505S :

Controller ROM Ver. 1.12.32

“S” included in a product name indicates that the machine has not a FAX function.

The S model of C505 has optional hard disks. However, the TOE is the targeted MFD model with which an optional hard disk is not equipped.

Whether a machine is the TOE can be distinguished by the product name that is displayed on the control panel when the machine is turned on. If “S” does not follow “C505” in the product name, the machine is not the TOE.

Users can confirm the hard disk equipment by the Configuration Report.

1.3. TOE Overview

1.3.1. TOE Type and Major Security Features

1.3.1.1. TOE Type

This TOE, categorized as an IT product, is the VersaLink C505 (hereinafter referred to as “MFD”) which has the copy, print, and network scan functions.

The TOE is the product which controls the whole MFD and protects the data that are transmitted over the encryption communication protocols.

These protocols protect the security of the TOE setting data, the security audit log data and the document data on the internal network between the TOE and the remote.

The TOE also prevents the document data and the used document data in the eMMC memory from being disclosed by unauthorized person.

1.3.1.2. Function Types

Table 1 shows the function types and functions provided by the TOE.

Table 1: Function Types and Functions provided by the TOE

| Function types | Functions provided by the TOE |
|-------------------|--|
| Basic Function | <ul style="list-style-type: none"> - Control Panel - Copy - Print - Network Scan - Embedded Web Server |
| Security Function | <ul style="list-style-type: none"> - Flash Memory Data Encryption - User Authentication - Administrator's Security Management - Customer Engineer Operation Restriction - Security Audit Log - Internal Network Data Protection - Self Test |

- To use print functions, the printer driver shall be installed to the external client for general user and that for system administrator.
- There are two types of user authentication, local authentication and remote authentication, and the TOE behaves with either one of the authentication types depending on the setting.

In this ST, the difference of the TOE behavior is described if the TOE behaves differently depending on the type of authentication being used. Unless specified, the behavior of the TOE is the same for both authentication types.

There are two types of remote authentication: LDAP authentication and Kerberos

authentication.

Note)

- Since the TOE's functions to print from USB and store to USB are set to disabled, they are not included in the target of evaluation. Therefore, the [Store to USB] and [Media Print] buttons do not appear on the control panel.

1.3.1.3. Usage and Major Security Features of TOE

The TOE is mainly used to perform the following functions:

- Copy function and Control Panel function are to read the original data from IIT and print them out from IOT according to the general user's instruction from the control panel. When more than one copy of an original data is ordered, the data read from IIT are first stored into the MFD eMMC memory. Then, the stored data are read out from the eMMC memory for the required number of times so that the required number of copies can be made.
- Print function is to decompose and print out the print data transmitted by a general user client.
- Embedded Web Server enables a system administrator to refer to and rewrite TOE setting data via Web browser.
- Network Scan function and Control Panel function are to read the original data from IIT and transmit the document data to FTP server, or Mail server, according to the information set in the MFD. This function is operated according to the general user's instruction from the control panel.

The TOE provides the following security features:

(1) Flash Memory Data Encryption

The document data and the security audit log data are encrypted before being stored into the eMMC memory when using any function of copy, print, etc. or configuring various security function settings.

(2) User Authentication

Access to the TOE functions is restricted to the authorized user and this function identifies and authenticates users. This function identifies and authenticates a user using his/her ID and password entered from the control panel or Embedded Web Server of a general user client, and enables access control over use of the TOE.

When a print job is received from a user client, the TOE identifies a registered user ID and stores the print job, without authenticating the user.

(3) System Administrator's Security Management

This function allows only the system administrator identified and authorized from the control panel or system administrator client to refer to and change the TOE security function settings.

(4) Customer Engineer Operation Restriction

A system administrator can prohibit CE from referring to and changing the TOE security function settings.

(5) Security Audit Log

The important events of TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who used what function.

(6) Internal Network Data Protection

This function protects the communication data on the internal network such as document data, security audit log data, and TOE setting data. (The following general encryption communication- protocols are supported: TLS, IPSec, and S/MIME.)

(7) Self Test

This function verifies the integrity of TSF executable code and TSF data.

1.3.2. Environment Assumptions

This TOE is assumed to be used as an IT product at general office and to be connected to user clients, and the internal network protected from threats on the external network by firewall etc.

Figure 1 shows the general environment for TOE operation.

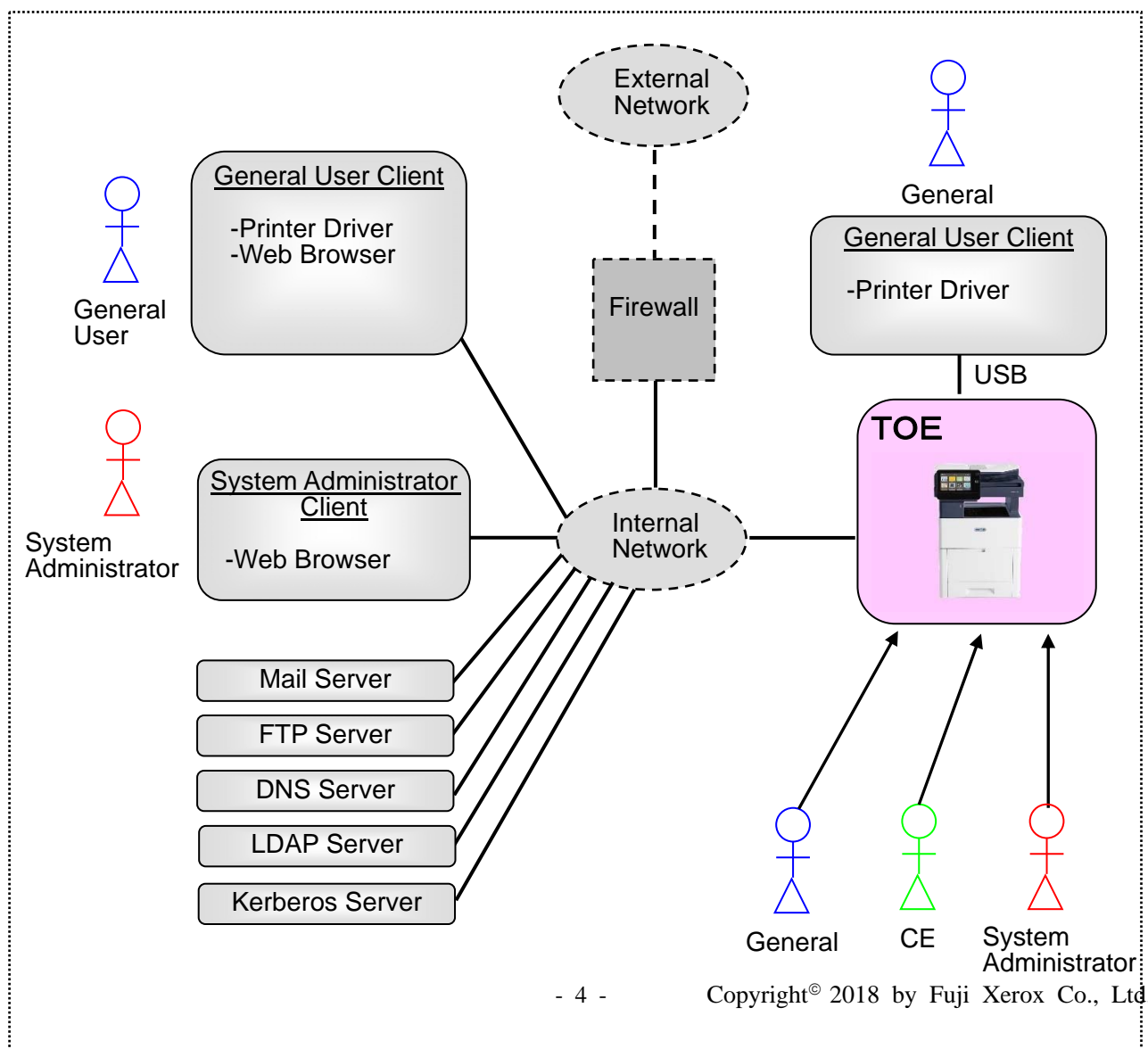


Figure 1: General Operational Environment

1.3.3. Required Non-TOE Hardware and Software

In the operational environment shown in Figure 1, the TOE (MFD) and the following non-TOE hardware/software exist.

(1) General user client:

The hardware is a general-purpose PC. When a client is connected to the MFD via the internal network and when the printer driver is installed to the client, the general user can request the MFD to print.

When the client is connected to the MFD directly via USB and printer is installed to the client, the user can request the MFD to print the document data.

(2) System administrator client:

The hardware is a general-purpose PC. A system administrator can refer to and change TOE setting data via Web browser.

(3) Mail server:

The hardware/OS is a general-purpose PC or server. The MFD sends/receives document data to/from Mail server via mail protocol.

(4) FTP server:

The hardware/OS is a general-purpose PC or server. The MFD sends document data to FTP server via FTP.

(5) DNS server:

The hardware/OS is a general-purpose PC or server. The MFD retrieves an IP address from the DNS server using the DNS protocol.

(6) LDAP server

The hardware/OS is a general-purpose PC or server. The MFD acquires identification and authentication information from LDAP server via LDAP. In addition, it acquires SA information of user role assumptions.

(7) Kerberos server

The hardware/OS is a general-purpose PC or server. The MFD acquires identification and authentication information from Kerberos server via Kerberos.

The OS of (1) general user client and (2) system administrator client are assumed to be

Windows 7 and Windows 8.1.

The (1) General user client uses "PCL6 Driver – Xerox User Interface – Microsoft Certified" as a printer driver.

The (6) LDAP server and (7) Kerberos server are assumed to be Windows Active Directory.

1.4. TOE Description

This section describes user assumptions and logical/physical scope of this TOE.

1.4.1. User Assumptions

Table 2 specifies the roles of TOE users assumed in this ST.

Table 2: User Role Assumptions

| Persons concerned | | Role Description |
|-----------------------------------|---|---|
| Administrator of the organization | | An administrator or responsible official of the organization which owns and uses TOE. |
| User | General user | A user of TOE functions such as copy, and print. |
| | System administrator (Key operator + System Administrator Privilege [SA]) | A user who is authorized to manage the device using the system administrator mode. A system administrator can refer to and rewrite the TOE setting for device operation and that for security functions via TOE control panel, and Web browser. |
| Customer engineer (CE) | | A user who can configure the TOE operational settings using the interface for CE. |

1.4.2. Logical Scope and Boundary

The logical scope of this TOE consists of each function of the programs recorded on the controller ROM.

Figure 2 shows the logical architecture of the MFD.

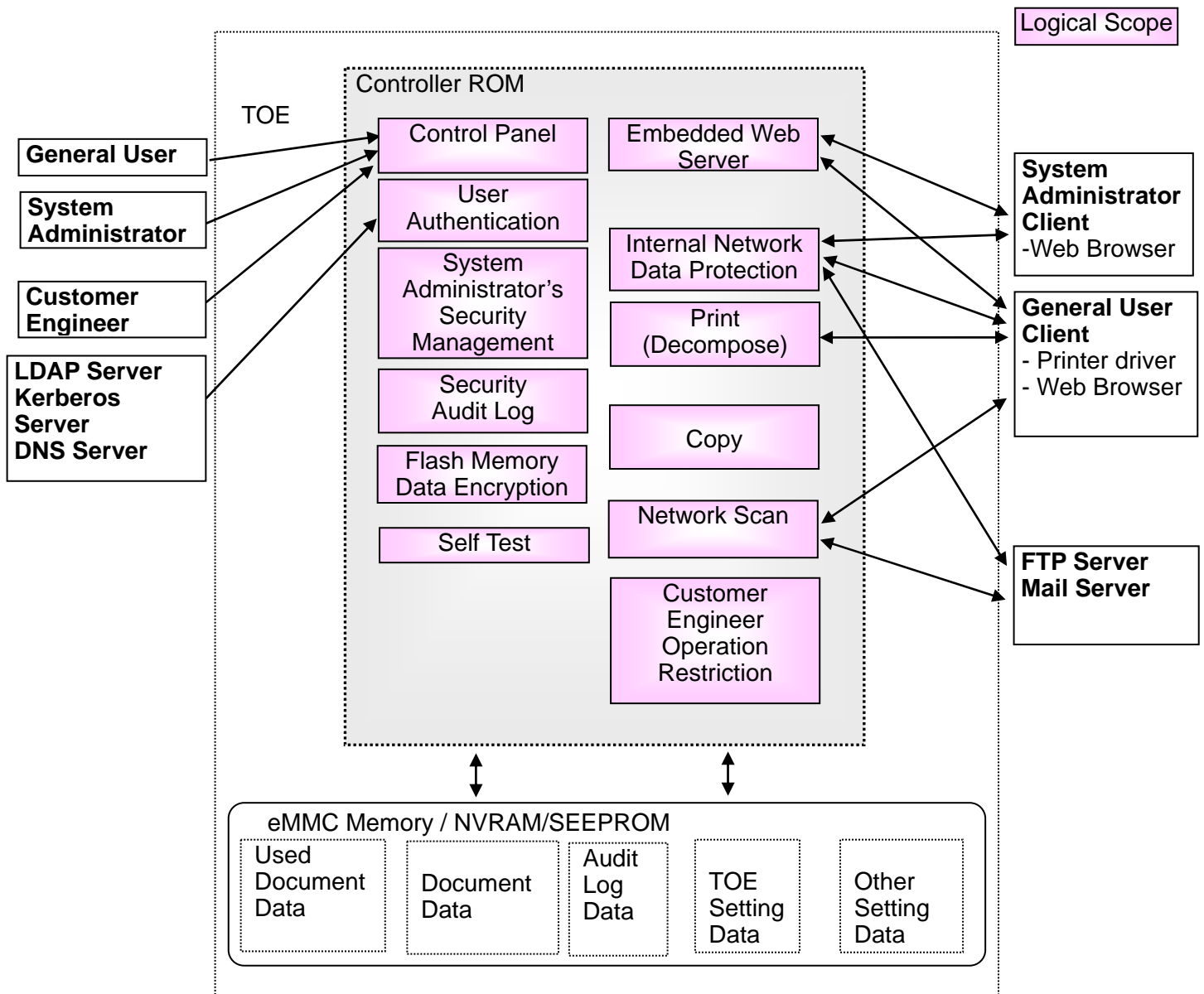


Figure 2: MFD Units and TOE Logical Scope

1.4.2.1. Basic Functions

As shown in Table 3, the TOE provides the functions of control panel, copy, print, network scan, and Embedded Web Server to general user.

Table 3: TOE Basic Functions

| Function | Description |
|------------------------|--|
| Control Panel Function | Control panel function is a user interface function for general user, CE, and system administrator to operate MFD functions. |
| Copy Function | Copy function is to read the original data from IIT and print them out |

| | |
|------------------------------|---|
| | <p>from IOT according to the general user's instruction from the control panel.</p> <p>When more than one copy of an original is ordered, the data read from IIT are first stored into the MFD eMMC memory. Then, the stored data are read out from the eMMC memory for the required number of times so that the required number of copies can be made.</p> |
| Print Function | <p>Print function is to print out the data according to the instruction from a general user client. The print data created via printer driver are sent to the MFD to be analyzed, decomposed, and printed out from IOT.</p> <p>The print function is of two types: the normal print in which the data are printed out from IOT directly after decomposed and the Store Print in which the bitmap data are temporarily stored in the eMMC memory and then printed out from IOT according to the general user's instruction from the control panel.</p> |
| Network Scan Function | <p>Network scan function is to read the original data from IIT and automatically transmit them to a general user client, FTP server, or Mail server according to the information set in the MFD. A general user can request this function from the control panel.</p> |
| Embedded Web Server Function | <p>A system administrator can access and rewrite TOE setting data. For this, a system administrator must be authenticated by his/her ID and password entered from Web browser of a system administrator client.</p> |

1.4.2.2. Security Functions

The security functions provided by the TOE are the following.

(1) Flash Memory Data Encryption

Some data such as the security audit log data remain in the eMMC memory even if the machine is powered off. To solve this problem, the document data and security audit log data are encrypted before being stored into the eMMC memory when operating any function of copy, print, and network scan, or configuring various security function settings.

(2) User Authentication

Access to the TOE functions is restricted to the authorized user.

A user needs to enter his/her ID and password from the Web browser of the general user client, or MFD control panel.

Only the authenticated user can use the following functions:

a) Functions controlled by the MFD control panel:

Copy, network scan, and print (This print function requires the Store Print preset from printer driver. A user must be authenticated from the control panel for print job.)

b) Functions controlled by Embedded Web Server:

Display of device condition, display of job status and its log.

Among the above functions which require user authentication, some particularly act as security functions. The following are the security functions which prevent the unauthorized reading of document data in the eMMC memory by an attacker who is impersonating an authorized user:

- The Store Print function which require user authentication from the control panel.

Figure 3 shows the authentication flow of the above functions.

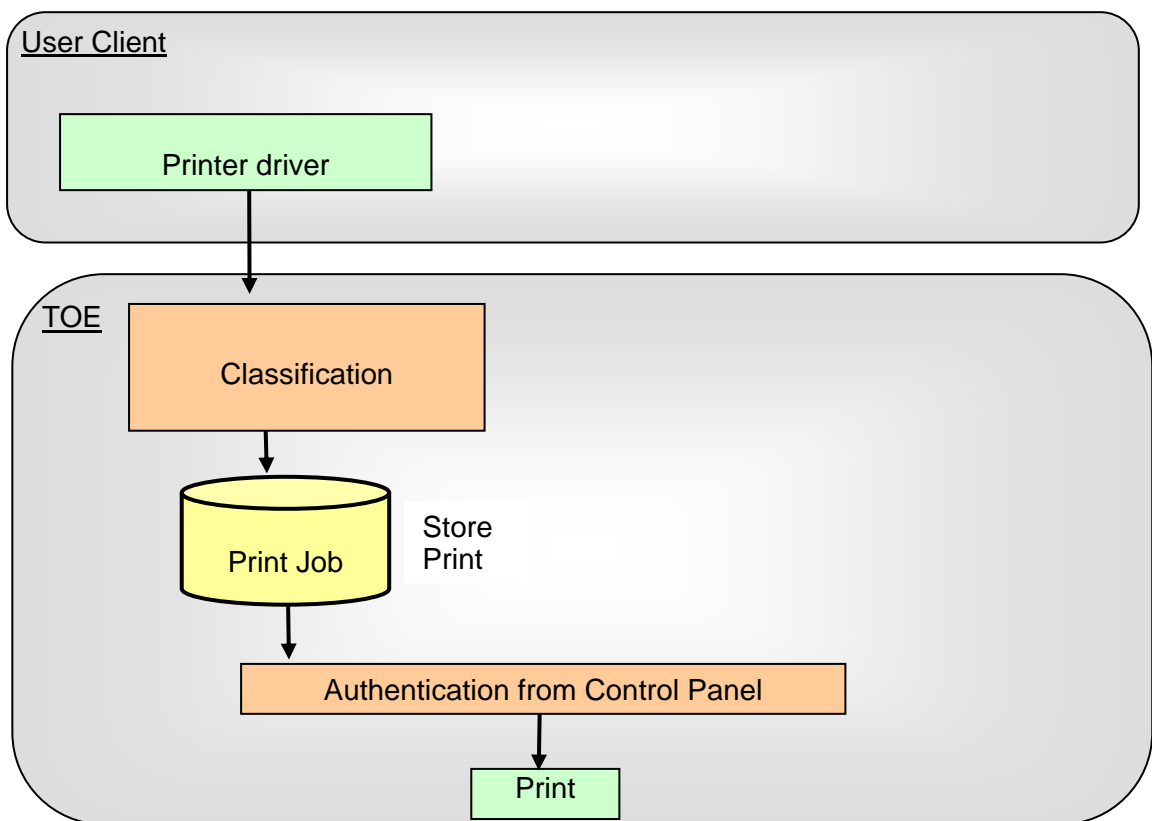


Figure 3: Authentication Flow for Store Print

- **Store Print Function**

When a user sends a print request from the printer driver in which the Store Print is preset, the print data are decomposed into bitmap data, classified according to the user ID, and temporarily stored in the corresponding Store Print area within the eMMC memory.

To refer to the stored print data, a user needs to enter his/her ID and password from the control panel. When the user is authenticated, the data on the waiting list corresponding to the user ID are displayed. The user can request printing or deletion of the data on the list.

(3) **System Administrator's Security Management**

To grant a privilege to a specific user, this TOE allows only the authenticated system

administrator to access the System Administrator mode which enables him/her to refer to and set the following security functions from the control panel:

- Refer to and set the Time/Date;
- Refer to and set the TLS communication;

Additionally, this TOE allows only the system administrator, who is authenticated from the system administrator client via Web browser using Embedded Web Server, to refer to and set the following security functions via Embedded Web Server:

- Refer to and set the Time/Date;
- Refer to and set the Self Test;
- Set the password of key operator (only a key operator is privileged);
- Refer to and set the ID of SA / general user and set the password(with local authentication only);
- Refer to and set the access denial when system administrator's authentication fails;
- Refer to and set the limit of user password length (with local authentication only);
- Refer to and set the Security Audit Log;
- Refer to and set the TLS communication;
- Refer to and set the IPSec communication;
- Refer to and set the S/MIME communication;
- Create/upload/download an X.509 certificate;
- Refer to and set the User Authentication;
- Refer to and set the general user permission;
- Refer to and set the Customer Engineer Operation Restriction

(4) Customer Engineer Operation Restriction

This TOE allows only the authenticated system administrator to refer to or enable/disable the Customer Engineer Operation Restriction setting from the Embedded Web Server. For this, CE cannot refer to or change the setting of each function described in (3) System Administrator's Security Management.

(5) Security Audit Log

The important events of TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function. Only a system administrator can supervise or analyze the log data by downloading them in the form of tab-delimited text file via Web browser using Embedded Web Server. To download the log data, TLS communication needs to be enabled.

(6) Internal Network Data Protection

The communication data on the internal network such as document data, security audit log

data, and TOE setting data are protected by the following general encryption communication-protocols:

- TLS
- IPSec
- S/MIME

(7) Self Test

This TOE can execute the self test function to verify the integrity of TSF executable code and TSF data.

1.4.2.3. Settings for the Secure Operation

System administrator shall set the following to enable security functions in 1.4.2.2.

- Access denial when system administrator's authentication fails
Default [5] Times.
- User Passcode Minimum Length
Set to [9] characters
- TLS
Set to [Enabled]
- IPSec
Set to [Enabled]
- S/MIME
Set to [Enabled]
- User Authentication
Set to [Local Authentication] or [Remote Authentication]
- Store Print
Set to [authority of user to only Store Print]
- Audit Log
Set to [Enabled]
- Customer Engineer Operation Restriction
Set to [Enabled]
- Self Test
Set to [Enabled]

1.4.3. Physical Scope and Boundary

The physical scope of this TOE is the MFD. Figure 4 shows configuration of each unit and TOE physical scope.

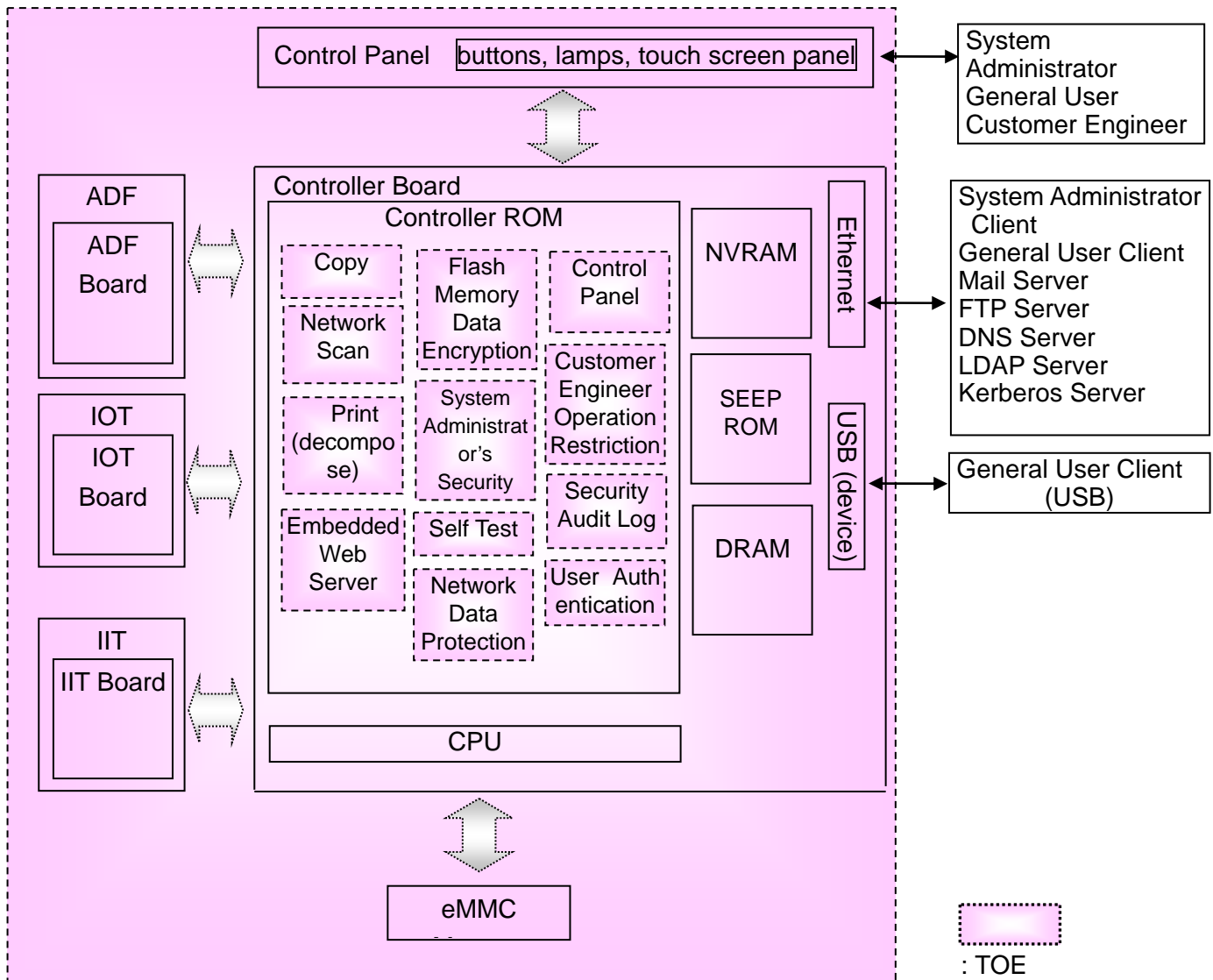


Figure 4: MFD Units and TOE Physical Scope

The MFD consists of the controller board and control panel, IIT, and IOT, ADF, and eMMC Memory.

The controller board is connected to the control panel via the internal interfaces which transmit control data, and the controller board is connected to the IIT board, and IOT board via the internal interfaces which transmit document data and control data.

The controller board is a PWB which controls MFD functions of copy, print, and network scan. The board has a network interface (Ethernet), and local interfaces (USB) and is connected to the IIT board and IOT board.

The control panel is a panel on which buttons, lamps, and a touch screen panel are mounted

to use and configure MFD functions of copy, print, and network scan.

The IIT (Image Input Terminal) is a device to scan an original and send its data to the controller board for copy, and network scan.

The IOT (Image Output Terminal) is a device to output image data which was sent from the controller board.

The ADF (Auto Document Feeder) is a device to automatically transfer original documents to IIT.

1.4.4. Guidance

The following are the guidance documents for this TOE.

- Xerox VersaLink C505 Color Multifunction Printer User Guide: Version 2.0 January 2018
(SHA256 Hash value:
1aa645e5355730c38fa3b3a4b3ffea7702dac46fa4bd668ee061230d92fc310c)
- Xerox VersaLink Series Multifunction and Single Function Printers System Administrator Guide: Version 2.0 October 2017
(SHA256 Hash value:
55ec10501077ecf5434d2663b080caa91d3ad8b30b612d008afb7e3f79545b50)
- Xerox VersaLink C505/C605/B605/B615 Multifunction Printer Security Function Supplementary Guide: Version 1.0, July 2018
(SHA256 Hash value:
7c7c7bc3e548b404cd5672861fe75eb6213a183e1ecd088e408122630ed92464)

2. CONFORMANCE CLAIMS

2.1. CC Conformance Claims

This ST and TOE conform to the following evaluation standards for information security (CC):

Common Criteria for Information Technology Security Evaluation

Part 1: Introduction and general model, Version 3.1 Revision 4 Japanese Version 1.0

Part 2: Security functional components, Version 3.1 Revision 4 Japanese Version 1.0

Part 3: Security assurance components, Version 3.1 Revision 4 Japanese Version 1.0

The security functional requirements of this ST conform to CC Part 2.

The security assurance requirements of this ST conform to CC Part 3.

2.2. PP Claims, Package Claims

2.2.1. PP Claims

There is no applicable Protection Profile.

2.2.2. Package Claims

This Security Target claims EAL2 augmented by ALC_FLR.2.

2.2.3. Conformance Rationale

There is no applicable PP rationale since this ST does not conform to PP.

3. SECURITY PROBLEM DEFINITION

This chapter describes the threats, organizational security policies, and the assumptions for the use of this TOE.

3.1. Threats

3.1.1. Assets Protected by TOE

This TOE protects the following assets (Figure 5):

(1) Right to use MFD functions

The general user's right to use each function of the TOE is assumed as an asset to be protected.

(2) Document data stored for job processing

When a general user uses MFD functions of copy, print, and network scan, the document data are temporarily stored in the eMMC memory for image processing, transmission, and Store Print. The stored data include general user's confidential information and are assumed as assets to be protected.

(3) Used document data

When a general user uses MFD functions of copy, print, and network scan, the document data are temporarily stored in the eMMC memory for image processing, transmission, and Store Print. When the jobs are completed or canceled, only the management information is deleted but the data itself remains. The residual data include general user's confidential information and are assumed as assets to be protected.

(4) Security audit log data

In the function of Security Audit Log, the important events such as device failure, configuration change and user operation are recorded in the eMMC memory based on when and who operated what function. For preventive maintenance and response to the events and detection of unauthorized access, only a system administrator can retrieve the log data stored in MFD by Embedded Web Server.

The log data are assumed as assets to be protected.

(5) TOE setting data

A system administrator can set TOE security functions from the MFD control panel or system administrator client by the function of System Administrator's Security Management. The setting data stored in the TOE (see Table 4) can be a threat to other assets if used without authorization and are assumed as assets to be protected.

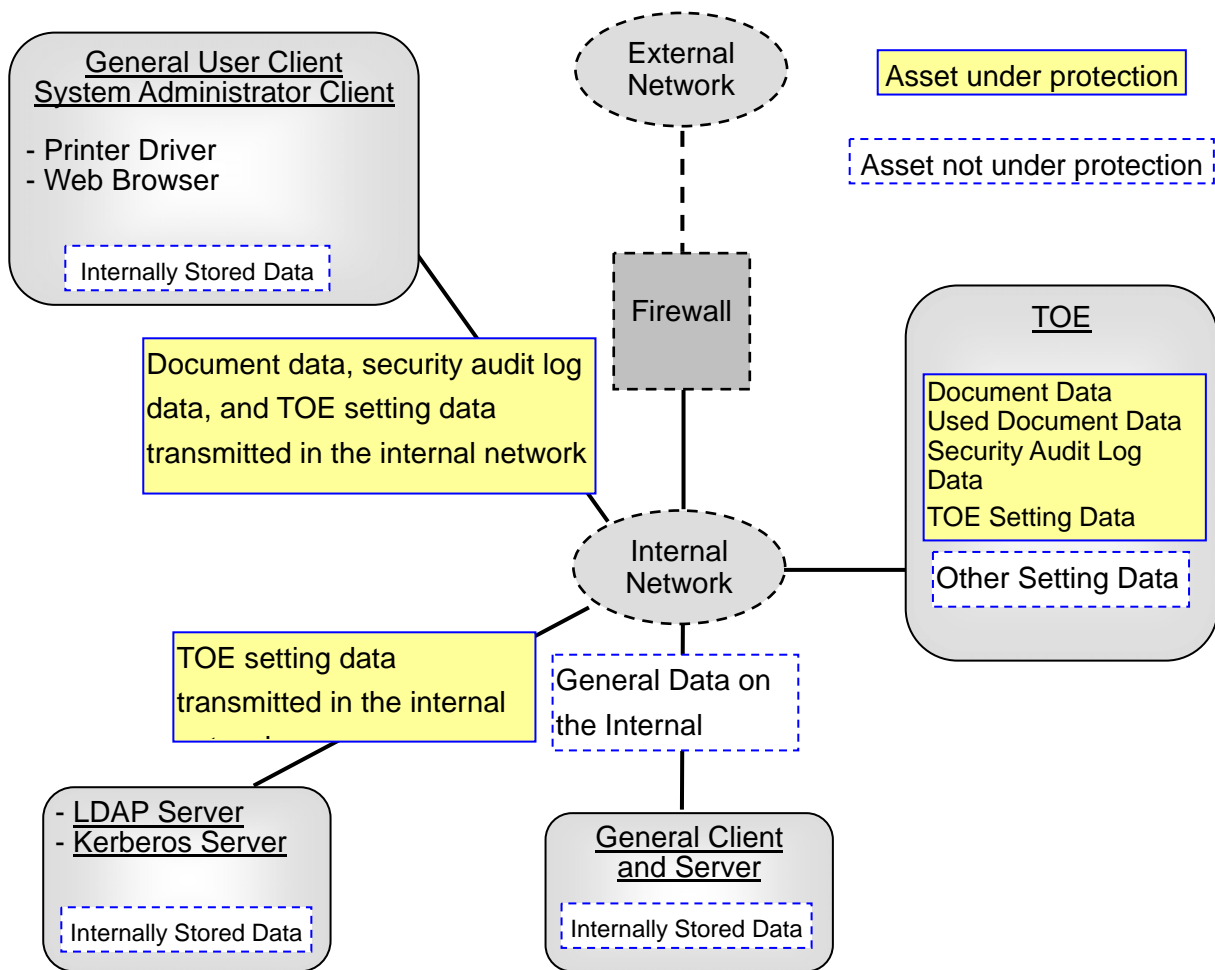


Figure 5: Assets under and not under Protection

Table 4 categorizes the TOE setting data recorded on NVRAM(Include eMMC memory) and SEEPROM of the controller board.

Table 4: Categories of TOE Setting Data

| Categories of TOE Setting Data (Note) |
|--|
| Data on minimum password length of user password |
| Data on password of key operator |
| Data on ID and password of SA/General user |
| Data on access denial due to authentication failures of system administrator |
| Data on Customer Engineer Operation Restriction |
| Data on Internal Network Data Protection |
| Data on Security Audit Log |
| Data on user permission |

| Categories of TOE Setting Data (Note) |
|---------------------------------------|
| Data on User Authentication |
| Data on date and time* |
| Data on Self Test |

Note: The setting data other than TOE setting data are also stored on NVRAM (Include eMMC memory) and SEEPROM. Those setting data, however, are not assumed as assets to be protected because they do not engage in TOE security functions.

* However, the present time data are not included.

3.1.2. Threats

Table 5 identifies the threats addressed by the TOE. An attacker is considered to have the disclosed information on TOE operations and low-level attack capability.

Table 5: Threats Addressed by the TOE

| Threat (Identifier) | Description |
|---------------------|--|
| T.CONFDATA | An attacker may access, read, or alter from control panel or system administrator client, the TOE setting data which only a system administrator is allowed to access. |
| T.DATA_SEC | An attacker may read or alter document data and security audit log data from control panel or Web browser without authorization. |
| T.COMM_TAP | An attacker may intercept or alter document data, security audit log data, and TOE setting data on the internal network. |
| T.CONSUME | An attacker may access the TOE and use TOE functions without authorization. |

3.2. Organizational Security Policies

Table 6 below describes the organizational security policy the TOE must comply with.

Table 6: Organizational Security Policy

| Organizational Policy (Identifier) | Description |
|---------------------------------------|--|
| P.VERIFY | The TOE shall execute self-test to verify the integrity of TSF executable code and TSF data. |
| P.CIPHER | The TOE shall encrypt the document data and the security audit log data in the eMMC memory. (A cryptographic key does not need to be destructed.) |

3.3. Assumptions

Table 7 shows the assumptions for the operation and use of this TOE.

Table 7: Assumptions

| Assumption (Identifier) | Description |
|----------------------------|--|
| Personnel Confidence | |
| A.ADMIN | A system administrator shall have the necessary knowledge of TOE security functions to perform the given role of managing the TOE and shall not operate the TOE with malicious intent. |
| A.USER | TOE users shall be trained and have competence about the TOE operation and precautions according to the policies of their organization and the product guidance. |
| Protection Mode | |
| A.SECMODE | A system administrator shall configure and set the TOE properly according to the security policy of organization and the product guidance document to manage the TOE and its external environment. |
| A.ACCESS | The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. |

4. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and for the environment and the rationale.

4.1. Security Objectives for the TOE

Table 8 defines the security objectives to be accomplished by the TOE.

Table 8: Security Objectives for the TOE

| Security Objectives(Identifier) | Description |
|---------------------------------|--|
| O.AUDITS | The TOE must provide the Security Audit Log function and its log data which are necessary to monitor unauthorized access. |
| O.CIPHER | The TOE must encrypt the document data and security audit log data to be stored into the eMMC memory. |
| O.COMM_SEC | The TOE must provide encryption communication function to protect the document data, security audit log data, and TOE setting data on the internal network between TOE and the remote from interception and alteration. |
| O.MANAGE | The TOE must inhibit a general user from accessing the TOE setting data. The TOE allows only the authenticated system administrator to access the system administrator mode which enables him/her to configure the security functions. |
| O.USER | The TOE must provide the function to identify TOE user and allow only the authorized user to retrieve, and delete the document data and to change the password. |
| O.RESTRICT | The TOE must inhibit an unauthorized user from using the TOE functions. |
| O.VERIFY | The TOE must provide self-test function to verify the integrity of TSF executable code and TSF data. |

4.2. Security Objectives for the Environment

Table 9 defines the security objectives for the TOE environment.

Table 9: Security Objectives for the Environment

| Security Objectives(Identifier) | Description |
|---------------------------------|---|
| OE.ADMIN | A system administrator who is assigned by an organization administrator as an appropriate and reliable person for this TOE management and who receives necessary training to manage the TOE. |
| OE.USER | The system administrator shall ensure that users have competence by training users about the TOE operation and precautions according to the policies of their organization and the product guidance. |
| OE.SEC | A system administrator shall configure and set the TOE properly according to the security policy of organization and the product guidance document to manage the TOE. In addition, a system administrator shall manage the external IT environment according to the security policy of organization and the product guidance document. |
| OE.PHYSICAL | The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE. |

4.3. Security Objectives Rationale

The security objectives are established to correspond to the assumptions specified in Security Problem Definition, to counter the threats, or to realize the organizational security policies. Table 10 shows assumptions / threats / organizational security policies and the corresponding security objectives. Moreover, Table 11 shows that each defined security problem is covered by the security objectives.

Table 10: Assumptions / Threats / Organizational Security Policies and the Corresponding Security Objectives

| Security Problems \ Security Objectives | A.ADMIN | A.USER | A.SECMODE | A.ACCESS | T.CONFDATA | T.COMM_TAP | T.DATA_SEC | T.CONSUME | P.VERIFY | P.CIPHER |
|---|---------|--------|-----------|----------|------------|------------|------------|-----------|----------|----------|
| O.AUDITS | | | | | ✓ | | ✓ | | | |
| O.CIPHER | | | | | | | | | | ✓ |
| O.COMM_SEC | | | | | | ✓ | | | | |
| O.MANAGE | | | | | ✓ | | ✓ | | | |
| O.VERIFY | | | | | | | | | ✓ | |
| O.USER | | | | | ✓ | | ✓ | | | |
| O.RESTRICT | | | | | | | | ✓ | | |
| OE.ADMIN | ✓ | | | | | | | | | |
| OE.USER | | ✓ | | | | | | | | |
| OE.SEC | | | ✓ | | ✓ | ✓ | ✓ | | ✓ | |
| OE.PHYSICAL | | | | ✓ | | | | | | |

Table 11: Security Objectives Rationale for Security Problem

| Security Problem | Security Objectives Rationale |
|------------------|--|
| A.ADMIN | By satisfying the following objective, A.ADMIN can be realized: By OE.ADMIN, a system administrator is assigned by an organization administrator as an appropriate and reliable person for this TOE management, and receives necessary training to manage the TOE and performs the TOE management according to the guidance. |
| A.USER | By satisfying the following objective, A.USER can be realized: By OE.USER, a system administrator trains users about the TOE operation and precautions according to the policies of their organization and the product guidance, and users have competence. |
| A.SECMODE | By satisfying the following objectives, A.SECMODE can be realized: By OE.SEC, a system administrator shall configure and set the TOE properly according to the security policy of organization and the product guidance document to manage the TOE. In addition, a system administrator shall manage the external IT environment according to the security policy of organization and the product guidance document. |

| Security Problem | Security Objectives Rationale |
|------------------|--|
| A.ACCESS | <p>By satisfying the following objective, A.ACCESS can be realized:</p> <p>By OE.PHYSICAL, a system administrator places the TOE in a secure or monitored area that provides protection from unmanaged physical access to the TOE.</p> |
| T.CONFDATA | <p>By satisfying the following objective, T.CONFDATA can be countered:</p> <p>By OE.SEC, it is necessary to enable the security functions (i.e. User Authentication with Password, System Administrator Password, Access Denial due to Authentication Failures, Customer Engineer Operation Restriction, and Security Audit Log) and permits only the authenticated system administrator to change the TOE setting data. In addition, it is necessary to manage the external IT environment according to the security policy of organization and the product guidance document.</p> <p>To be specific, this threat can be countered by the following security objectives, O.MANAGE, O.USER, and O.AUDITS:</p> <p>By O.MANAGE, only the authenticated system administrator is allowed to enable/disable the TOE security functions and to refer to / update the TOE setting data.</p> <p>By O.USER, only the authorized user is allowed to change the password.</p> <p>By O.AUDITS, the audit log function necessary to monitor unauthorized access and the security audit log data are provided.</p> |
| T.CONSUME | <p>By satisfying the following objective, T.CONSUME can be countered.</p> <p>By O.RESTRICT, the access to the TOE can be controlled.</p> |
| T.COMM_TAP | <p>By satisfying the following objectives, T.COMM_TAP can be countered.</p> <p>By OE.SEC, the document data, security audit log data, and TOE setting data on the internal network can be protected from interception.</p> <p>By O.COMM_SEC, the client/server authentication function of encryption communication protocol allows only the authorized user to send/receive the communication data. Encrypting communication data with encryption function also disables the interception and alteration of the internal network data (incl. document data, security audit log data, and TOE setting data).</p> |
| T.DATA_SEC | <p>By satisfying the following objectives, T.DATA_SEC can be countered.</p> <p>By OE.SEC, it is necessary to enable the following passwords, user authentication function, and security audit log function: User Password, System Administrator Password, Local Authentication or</p> |

| Security Problem | Security Objectives Rationale |
|------------------|--|
| | <p>Remote Authentication, Security Audit Log. Then, only the authenticated user is allowed to access the security audit log data and document data. In addition, it is necessary to manage the external IT environment according to the security policy of organization and the product guidance document.</p> <p>By O.USER, only the authenticated user is allowed to read out or delete the document data and security audit log data stored in the eMMC memory.</p> <p>By O.MANAGE, only the authenticated system administrator is allowed to configure the TOE security functions.</p> <p>By O.AUDITS, the audit log function necessary to monitor unauthorized access and the security audit log data are provided.</p> |
| P. VERIFY | <p>By satisfying the following objectives, P .VERIFY can be observed.</p> <p>By OE.SEC, it is necessary to enable the following security function, and execute self-test to verify the integrity of TSF executable code and TSF data.</p> <p>-Self Test</p> <p>The TOE can execute the self test function to verify the integrity of TSF executable code and TSF data.</p> |
| P.CIPHER | <p>By satisfying the following objective, O.CIPHER can be countered.</p> <p>-Flash Memory Data Encryption</p> <p>This function makes unauthorized reading of document data or security audit log data impossible by encrypting the document data or security audit log data stored in the eMMC memory.</p> <p>By satisfying this policy, P.CIPHER can be observed.</p> |

5. EXTENDED COMPONENTS DEFINITION

5.1. Extended Components

This ST conforms to CC Part 2 and CC Part 3, and there are no extended components which shall be defined.

6. SECURITY REQUIREMENTS

This chapter describes the security functional requirements, security assurance requirements, and security requirement rationale.

The terms and phrases used in this chapter are defined below.

- Subject

| Term/phrase | Definition |
|--|--|
| System Administrator Process | Operation upon using Store Print when the user authentication of System Administrator succeeded. |
| General User Process | Operation upon using Store Print when the user authentication of general user succeeded. |
| Sending information to the internal network | To send the Network Scan data to the destination, a client PC, within the internal network. |
| Receiving information from the internal network. | To receive the print data from a client PC, within the internal network. |

- Object

| Term/phrase | Definition |
|-------------------------|--|
| Store Print | A print function in which bitmap data (decomposed print data) are temporarily stored in the MFD eMMC memory and then printed out according to the authenticated general user's instruction from the control panel. |
| Document data | Document data means all the data including image data transmitted across the MFD when any of copy, print, or network scan functions is operated by a general user. |
| Security Audit Log Data | The chronologically recorded data of important events of the TOE. The events such as device failure, configuration change, and user operation are recorded based on when and who caused what event and its result. |

- Operation

| Term/phrase | Definition |
|--------------------|---|
| Modify of behavior | To change the settings of the following information: User Authentication (Local, Remote) Internal Network Data Protection (Certificate and encryption type) |

| | |
|--------|--|
| Modify | Changes of TSF data and security attributes (user identifier). |
|--------|--|

- Security attributes

| Term/phrase | Definition |
|---------------------------------|---|
| General User role | Indicates the authority required for general user to use the TOE. |
| System Administrator role | Indicates the authority required for System Administrator to use the TOE. |
| SA role | Indicates the authority required for SA to use the TOE. |
| Key Operator role | Indicates the authority required for key operator to use the TOE. |
| General User identifier | User ID used to authenticate and identify general user. |
| SA identifier | User ID used to authenticate and identify SA. |
| Key Operator identifier | User ID used to authenticate and identify key operator. |
| Owner identifier of Store Print | User ID of the user who sent a Store Print job. |

- Entity outside the TOE

| Term/phrase | Definition |
|-------------------------------------|--|
| System Administrator | This term covers both key operator and SA. |
| Key Operator | An authorized user who manages MFD maintenance and makes TOE security function settings. |
| System Administrator Privilege (SA) | The user(s) who manage MFD maintenance and configure TOE security functions. SA can be created/registered by key operator or the other SA who is already registered. |
| General User | Any person who uses copy, network scan, and print functions of MFD. |

- Other terminology

| Term/phrase | Definition |
|-----------------|---|
| SHA-2 algorithm | The FIPS-standard cryptographic hash function used for generation of a cryptographic key of eMMC Memory data. |
| AES | The FIPS-standard encryption algorithm used for encryption/decryption of eMMC memory data. |

| | |
|--|---|
| Access denial due to authentication failure of system administrator ID | When the number of unsuccessful authentication attempts has exceeded the specified number of times, Identification and authentication of relevant user is inhibited until the TOE is cycled. |
| Data on minimum user password length | Minimum user password length to set the User password from MFD control panel. Included in the TOE setting data. |
| Data on ID of key operator | ID data for key operator authentication. |
| Data on password of key operator | Password data for key operator authentication. Included in the TOE setting data. |
| Data on ID of SA | ID data for SA authentication. Included in the TOE setting data. |
| Data on password of SA | Password data for SA authentication. Included in the TOE setting data. |
| Data on ID of General User | ID data for general user authentication. Included in the TOE setting data. |
| Data on password of General User | Password data for general user authentication. Included in the TOE setting data. |
| Data on access denial due to authentication failures of system administrator | The data on whether to enable/disable access denial due to authentication failure of system administrator ID. They also incorporate the data on the allowable number of the failures before access denial. Included in the TOE setting data. |
| Data on Security Audit Log | The data on whether to enable/disable the function to trace/ record the important events of the TOE such as device failure, configuration change, and user operation, based on when and who operated what function. |
| Data on User Authentication | The data on whether to enable/disable the authentication function using the data on user authentication when copy, network scan, and print functions of MFD are used. It also incorporates the data on the setting. Included in the TOE setting data. |
| Data on User Permission | The data on authority of U.NORMAL. Included in the TOE setting data. |
| Data on Internal Network Data Protection | The data on whether to enable/disable the general encryption communication protocols to protect the communication data on the internal network such as document data, security audit log data, and TOE setting data. They also incorporate the data on the setting. Included in the TOE setting data. |

| | |
|---|---|
| Data on Customer Engineer Operation Restriction | The data on whether to enable/disable Customer Engineer Operation Restriction. Included in the TOE setting data. |
| Data on date and time | The data on the time zone / summer time information / present date and time.. Included in the TOE setting data. |
| Data on Self Test | The data on whether to enable/disable the functions related to Self Test. Included in the TOE setting data. |
| System Administrator mode | An operation mode that enables a system administrator to refer to and rewrite TOE setting for device operation and that for security functions according to the operational environment. This mode is distinguished from the operation mode that enables a general user to use the MFD functions. |
| Certificate | Defined in the X.509 which is recommended by ITU-T. The data for user authentication (name, identification name, organization where he/she belongs to, etc.), public key, expiry date, serial number, signature, etc. |
| Printer driver | Software to convert the data on a general user client into print data written in page description language (PDL), a readable format for MFD. Used on the user client. |

6.1. Security Functional Requirements

Security functional requirements which the TOE offers are described below. The security functional requirements are based on the class and component which are specified by the [CC part 2].

6.1.1. 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 [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
- c) [assignment: other specifically defined auditable events].

[selection, choose one of: minimum, basic, detailed, not specified]

- *not specified*

[assignment: other specifically defined auditable events]

- *the actions to be audited (defined by CC) and the corresponding auditable events (events to be recorded as execution log) of TOE.*

Shown in Table 12

Table 12: Auditable Events of TOE and Individually Defined Auditable Events

| Functional Requirements | Actions to be audited (defined by CC) | Auditable events of TOE |
|-------------------------|---|---|
| FAU_GEN.1 | None | - |
| FAU_SAR.1 | a) Basic: Reading of information from the audit records. | <i>Basic: Successful download of security audit log data.</i> |
| FAU_SAR.2 | a) Basic: Unsuccessful attempts to read information from the audit records. | <i>Basic: Unsuccessful download of security audit log data.</i> |
| FAU_STG.1 | None | - |
| FAU_STG.4 | a) Basic: Actions taken due to the audit storage failure. | <i>None</i> |
| FCS_CKM.1 | a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object | <i>None</i> |

| | | |
|-----------|--|--|
| | value(s) excluding any sensitive information (e.g. secret or private keys). | |
| FCS_COP.1 | a) Minimal: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes. | None |
| FDP_ACC.1 | None | - |
| FDP_ACF.1 | a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check. | <i>Basic: User name, job information, and success/failure regarding execution of Store Print.</i> |
| FIA_AFL.1 | a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal). | <i><Minimal> Authentication lock of system administrator Authentication failure</i> |
| FIA_ATD.1 | None | - |
| FIA_SOS.1 | a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics | <i><Individually defined auditable events> Registration of user and changes in user registration data (password)</i> |
| FIA_UAU.1 | a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism. c) Detailed: All TSF mediated actions performed before authentication of the user. | <i>< Basic > Success/failure of authentication</i> |
| FIA_UAU.7 | None | - |
| FIA_UID.2 | a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided. | <i>< Basic > Success/failure of authentication</i> |
| FIA_USB.1 | a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a | <i>< Basic > Registration of system</i> |

| | | |
|------------|---|---|
| | subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject). | <i>administrator, and changes in user registration data (role)</i> |
| FMT_MOF.1 | a) Basic: All modifications in the behavior of the functions in the TSF. | <i><Basic> Changes in security function configuration.</i> |
| FMT_MSA.1 | a) Basic: All modifications of the values of security attributes. | <i><Basic> User name, job information, and success/failure regarding execution of Store Print.</i> |
| FMT_MSA.3 | a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes. | <i>None</i> |
| FMT_MTD.1. | a) Basic: All modifications to the values of TSF data. | <i><Individually defined auditable events> Changes in registration data (password) of system administrator, and in the setting of security functions.</i> |
| FMT_SMF.1 | a) Minimal: Use of the management functions. | <i>< Minimal > Access to system administrator mode</i> |
| FMT_SMR.1 | a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role. | <i><Minimal> Registration of system administrator, changes in user registration data (role), and deletion of system administrator</i> |
| FPT_STM.1 | a) Minimal: changes to the time; b) Detailed: providing a timestamp. | <i><Minimal> Changes in time setting.</i> |
| FPT_TST.1 | a) Minimal: Termination of an interactive session by the session locking mechanism. | <i><Basic> Execution of Self Test and the test result</i> |
| FTP_ITC.1 | a) Minimal: Failure of the trusted channel | <i><Minimal></i> |

| | | |
|--|--|--|
| | <p>functions.</p> <p>b) Minimal: Identification of the initiator and target of failed trusted channel functions.</p> <p>c) Basic: All attempted uses of the trusted channel functions.</p> <p>d) Basic: Identification of the initiator and target of all trusted channel functions.</p> | <p><i>Failure of the trusted Communication within a specified period of time, and client host data (host name or IP address)</i></p> |
|--|--|--|

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, [assignment: other audit relevant information].

[assignment: other audit relevant information].

- none

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: authorized users] with the capability to read [assignment: list of audit information] from the audit records.

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

[assignment: authorized users]

- system administrator

[assignment: list of audit information]

- all log information

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 unauthorized deletion. |
| FAU_STG.1.2 | <p>The TSF shall be able to [selection, choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.</p> <p>[selection, choose one of: prevent, detect] - <i>prevent</i></p> |
| 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 | <p>The TSF shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorized 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.</p> <p>[selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorized user with special rights”, “overwrite the oldest stored audit records”] - <i>overwrite the oldest stored audit records</i> [assignment: other actions to be taken in case of audit storage failure] - <i>no other actions to be taken</i></p> |
| 6.1.2. Class FCS: | Cryptographic support |
| FCS_CKM.1 | Cryptographic key generation |
| Hierarchical to: | No other components |
| Dependencies: | <p>[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction</p> |

| | |
|-------------------|--|
| FCS_CKM.1.1 | <p>TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].</p> <p>[assignment: list of standards] - <i>FIPS PUB 180-2</i></p> <p>[assignment: cryptographic key generation algorithm] - <i>SHA-2</i> algorithm</p> <p>[assignment: cryptographic key sizes] - <i>256bits</i></p> |
| FCS_COP.1 | Cryptographic operation |
| Hierarchical to: | No other components |
| Dependencies: | <p>[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.4 Cryptographic key destruction</p> |
| FCS_COP.1.1 | <p>The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].</p> <p>[assignment: list of standards] - <i>FIPS PUB 197</i></p> <p>[assignment: cryptographic algorithm] - <i>AES</i></p> <p>[assignment: cryptographic key sizes] - <i>256bits</i></p> <p>[assignment: list of cryptographic operations] - <i>encryption of the document data and security audit log data to be stored in the eMMC memory and decryption of the document data and security audit log data retrieved from the eMMC memory.</i></p> |
| 6.1.3. 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 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[assignment: access control SFP]

- *MFD access control SFP*

[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

- *subjects, objects, and operations between subjects and objects listed in Table 13*

Table 13: Operations between Subjects and Objects Covered by MFD Access Control SFP

| Subject | Object | Operation |
|-------------------------------------|--------------------|----------------------------------|
| <i>System Administrator process</i> | <i>Store Print</i> | <i>Deletion of document data</i> |
| <i>General User Process</i> | | <i>Print of document data</i> |

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 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

[assignment: access control SFP]

- *MFD access control SFP*

[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

- *General user identifier corresponding to the general user process, System Administrator identifier corresponding to the System Administrator process*

- *Owner identifier of Store Print*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
 - the rules, shown in Table 14, for controlling the access among controlled subjects using the controlled operations on the controlled objects

Table 14: Rules for Access Control

| <i>Rules for Store Print Operation in the General User Process and System Administrator Process</i> | |
|---|--|
| - Deletion and print of document data When the general user identifier and System Administrator identifier of the general user process and System Administrator process match the owner identifier of Store Print, print and deletion of the document data inside are allowed. When the document data are deleted, the corresponding Store Print area is also deleted. | |

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
 - no rules that explicitly authorize the access

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
 - no rules that explicitly deny the access

6.1.4. Class FIA: Identification and authentication

FIA_AFL.1 (1) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 (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].

[assignment: list of authentication events]

- *key operator authentication*

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

- *[assignment: positive integer number]*

[assignment: positive integer number]

- 5

FIA_AFL.1.2 (1)

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]

- *Identification and authentication of key operator is inhibited until TOE is cycled*

FIA_AFL.1(2)

Authentication failure handling

Hierarchical to:

No other components

Dependencies:

FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 (2)

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].

[assignment: list of authentication events]

- *SA authentication (with local authentication)*

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

- *[assignment: positive integer number]*

[assignment: positive integer number]

- 5

FIA_AFL.1.2 (2)

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

| | |
|------------------|---|
| | actions]. |
| | [selection: met, surpassed] |
| | - <i>met</i> |
| | [assignment: list of actions] |
| | - <i>Identification and authentication of relevant user is inhibited until TOE is cycled.</i> |
| 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]. |
| | - <i>Key Operator role</i> |
| | - <i>SA role</i> |
| | - <i>General User role</i> |
| FIA_SOS.1 | Verification of secrets |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_SOS.1.1 | The TSF shall provide a mechanism to verify that secrets (user password when local authentication is used) meet [assignment: a defined quality metric]. |
| | [assignment: a defined quality metric]. |
| | - <i>Password length is restricted to 9 or more characters</i> |
| FIA_UAU.1 | Timing of authentication |
| Hierarchical to: | No other components |
| Dependencies: | FIA_UID.1 Timing of identification |
| FIA_UAU.1.1 | The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated. |
| | [assignment: list of TSF mediated actions] |
| | - <i>storing the print job delivered from user client</i> |
| 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] - <i>display of asterisks (“*”) to hide the entered password characters</i> |
| FIA_UID.2 | User identification before any action |
| Hierarchical to: | FIA_UID.1 Timing of identification |
| Dependencies: | No dependencies |
| FIA_UID.2.1 | 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]. - <i>Key Operator role</i> - <i>SA role</i> - <i>General User role</i> |
| 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]. - <i>none</i> |
| 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

6.1.5. 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 The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

[selection: determine the behavior of, disable, enable, modify the behavior of]

- enable, disable, or modify the behavior of

[assignment: list of functions]

- for security listed in Table 15

[assignment: the authorized identified roles]

- the roles listed in Table 15

Table 15: List of Security Functions

| Security Functions | Operations | Roles |
|---|--------------------------------|-----------------------------|
| <i>Access denial due to authentication failure of system administrator ID</i> | <i>enable, disable</i> | <i>System Administrator</i> |
| <i>User Authentication</i> | <i>enable, disable, modify</i> | <i>System Administrator</i> |
| <i>Security Audit Log</i> | <i>enable, disable</i> | <i>System Administrator</i> |
| <i>Internal Network Data Protection</i> | <i>enable, disable, modify</i> | <i>System Administrator</i> |
| <i>Customer Engineer Operation Restriction</i> | <i>enable, disable</i> | <i>System Administrator</i> |
| <i>Self Test</i> | <i>enable, disable</i> | <i>System Administrator</i> |

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] 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 authorized identified roles].

[assignment: access control SFP(s), information flow control SFP(s)]

- *MFD access control SFP*

[selection: change default, query, modify, delete, [assignment: other operations]]

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

[assignment: other operations]

- *create*

[assignment: list of security attributes]

- *user identifier, and Store Print owner identifier*

[assignment: the authorized identified roles].

- *the operations and roles listed in Table 16*

Table 16: Security Attributes and Authorized Roles

| Security Attribute | Operations | Roles |
|---|------------------------------|--|
| <i>Key operator identifier</i> | <i>query</i> | <i>System Administrator</i> |
| <i>SA identifier (with local authentication only)</i> | <i>query, delete, create</i> | <i>System Administrator</i> |
| <i>General user identifier (with local authentication only)</i> | <i>query, delete, create</i> | <i>System Administrator</i> |
| <i>Store Print owner identifier</i> | <i>query, delete, create</i> | <i>System Administrator General user</i> |

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 The TSF shall enforce the [assignment: access control SFP, information flow 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.

[assignment: access control SFP, information flow control SFP]

- *MFD access control SFP*

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

- *[assignment: other property]*

- *Initialization property in Table 17*

Table 17 Initialization property

| Object | Security Attributes | Default |
|--------------------|--|--|
| <i>store print</i> | <i>Owner identifier of store print</i> | <i>Creator's user identifier and available user identifier</i> |

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

[assignment: the authorized identified roles]

- *none*

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 The TSF shall restrict the ability to [selection: change default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

[selection: change default, query, modify, delete, clear, [assignment: other operations]]

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

[assignment: other operations]]

- *create*

[assignment: list of TSF data]

- *TSF data listed in Table 18*

[assignment: the authorized identified roles].

- *the roles listed in Table 18*

Table 18: Operation of TSF Data

| TSF Data | Operations | Roles |
|--|------------------------------|--|
| <i>Data on key operator Password</i> | <i>modify</i> | <i>Key operator</i> |
| <i>Data on SA ID (with local authentication only)</i> | <i>query, delete, create</i> | <i>System Administrator</i> |
| <i>Data on SA Password (with local authentication only)</i> | <i>modify</i> | <i>System Administrator</i> |
| <i>Data on General user ID (with local authentication only)</i> | <i>query, delete, create</i> | <i>System Administrator</i> |
| <i>Data on General user Password (with local authentication only)</i> | <i>modify</i> | <i>System Administrator General user</i> |
| <i>Data on User Authentication</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on minimum password length of user password (with local authentication only)</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on User permission</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on Access denial due to authentication failure of system administrator</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on Security Audit Log</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on Internal Network Data Protection</i> | <i>query, modify, delete</i> | <i>System Administrator</i> |
| <i>Data on Customer Engineer Operation Restriction</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on date and time</i> | <i>query, modify</i> | <i>System Administrator</i> |
| <i>Data on Self Test</i> | <i>query, modify</i> | <i>System Administrator</i> |

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 to be provided by the TSF].

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

- Security Management Functions listed in Table 19

Table 19: Security Management Functions Provided by TSF

| Functional requirements | Management items defined by CC | Management functions of TOE |
|-------------------------|--|---|
| FAU_GEN.1 | There are no management activities foreseen. | <i>Management of data on Security Audit Log settings</i> |
| FAU_SAR.1 | a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records. | <i>Management of data on key operator (password) Management of data on SA (ID and password) (with local authentication only)</i> |
| FAU_SAR.2 | None | - |
| FAU_STG.1 | None | - |
| FAU_STG.4 | a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure. | <i>None Reason: The control parameter of audit log is fixed and is not managed.</i> |
| FCS_CKM.1 | None | - |
| FCS_COP.1 | None | - |
| FDP_ACC.1 | None | - |
| FDP_ACF.1 | a) Managing the attributes used to make explicit access or denial based decisions. | <i>Management of owner identifier of store print Management of data on user permission</i> |
| FIA_AFL.1 | a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure. | <i>Management of allowable number of system administrator's authentication failures Management of Access Denial</i> |
| FIA_ATD.1 | a) if so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users. | <i>None Reason: There are no additional security attributes and there are no additional security attributes to be managed.</i> |
| FIA_SOS.1 | a) the management of the metric used to verify the secrets. | <i>- Management of data on minimum password length of user password</i> |
| FIA_UAU.1 | a) Management of the authentication data by an administrator; b) Management of the authentication data by the associated user; c) Managing the list of actions that can be taken before the user is authenticated. | <i>- Management of data on key operator(password) - Management of data on SA and general user (ID and password) (with local authentication only) - Management of data on user authentication.</i> |

| | | |
|------------|---|---|
| FIA_UAU.7 | None | - |
| FIA_UID.2 | a) The management of the user identities. | - Management of data on SA and general user (ID) (with local authentication only) - Management of data on user authentication. |
| FIA_USB.1 | a) an authorized administrator can define default subject security attributes. b) an authorized administrator can change subject security attributes. | None Reason: Action and security attributes are fixed and are not managed. |
| FMT_MOF.1 | a) Managing the group of roles that can interact with the functions in the TSF; | Management of data on Customer Engineer Operation Restriction |
| FMT_MSA.1 | a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values. | None Reason: The role group is fixed and is not managed. |
| FMT_MSA.3 | a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values. | None Reason: The role group is only a system administrator and is not managed. |
| FMT_MTD.1. | a) Managing the group of roles that can interact with the TSF data. | Management of data on Customer Engineer Operation Restriction |
| FMT_SMF.1 | None | - |
| FMT_SMR.1 | a) Managing the group of users that are part of a role. | None Reason: The role group is fixed and is not managed |
| FPT_STM.1 | a) management of the time. | Management of time and data. |
| FPT_TST.1 | a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) management of the time interval if appropriate. | Management of data on Self Test. |
| FTP_ITC.1 | a) Configuring the actions that require trusted channel, if supported. | Management of data on Internal Network Data Protection. |

| | |
|-------------------|---|
| FMT_SMR.1 | Security roles |
| Hierarchical to: | No other components |
| Dependencies: | FIA_UID.1 Timing of identification |
| FMT_SMR.1.1 | <p>The TSF shall maintain the roles [assignment: the authorized identified roles].</p> <p>[assignment: the authorized identified roles] <i>- system administrator, SA, general user</i></p> |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |
| 6.1.6. Class FPT: | Protection of the TSF |
| 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.1 | TSF testing |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_TST.1.1 | <p>The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].</p> <p>[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] <i>- at the conditions [assignment: conditions under which self test should occur]</i> [assignment: conditions under which self test should occur] <i>- at initiation under which self test is set</i> [selection: [assignment: parts of TSF], the TSF]. <i>- [assignment: parts of TSF]</i> <i>- TSF executable code</i></p> |
| FPT_TST.1.2 | The TSF shall provide authorised users with the capability to verify the |

integrity of [selection: [assignment: parts of TSF data], TSF data].

[selection: [assignment: parts of TSF data], TSF data]

- [assignment: parts of TSF data]

- *TSF data (excluding audit log data and present time data)*

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF].

[selection: [assignment: parts of TSF], TSF]

- *assignment: parts of TSF*

- *TSF executable code*

6.1.7. Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.

[selection: the TSF, another trusted IT product]

- *the TSF, another trusted IT product*

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

[assignment: list of functions for which a trusted channel is required].

- *TOE communication service via Web, communication service for printer driver, communication service for LDAP, communication service for Kerberos, communication service for SMTP, communication service for FTP, and communication service for DNS.*

6.2. Security Assurance Requirements

The requirements for the TOE security assurance are described in Table 20.

The evaluation assurance level of the TOE is EAL2.

The added security assurance component is ALC_FLR.2.

Table 20: Security Assurance Requirements

| Assurance Class | Assurance Component | |
|------------------------------------|---------------------|---|
| ADV: Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.2 | Security-enforcing functional specification |
| | ADV_TDS.1 | Basic design |
| AGD: Guidance documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.2 | Use of a CM system |
| | ALC_CMS.2 | Parts of the TOE CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_FLR.2 | Flaw reporting procedures |
| ASE: Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_TSS.1 | TOE summary specification |
| ATE: Tests | ATE_COV.1 | Evidence of coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing - sample |
| AVA: Vulnerability assessment | AVA_VAN.2 | Vulnerability analysis |

6.3. Security Requirement Rationale

6.3.1. Security Functional Requirements Rationale

Table 21 lists security functional requirements and the corresponding security objectives. As shown in Table 21, each security functional requirement corresponds to at least one security objective of the TOE.

Table 22 shows the rationale demonstrating that each security objective is assured by TOE security functional requirements.

Table 21: Security Functional Requirements and the Corresponding Security Objectives

| Security Objectives Security Functional Requirements | O.AUDITS | O.CIPHER | O.COMM_SEC | O.MANAGE | O.RESTRICT | O.USER | O.VERIFY |
|---|----------|----------|------------|----------|------------|--------|----------|
| FAU_GEN.1 | ✓ | | | | | | |
| FAU_SAR.1 | ✓ | | | | | | |
| FAU_SAR.2 | ✓ | | | | | | |
| FAU_STG.1 | ✓ | | | | | | |
| FAU_STG.4 | ✓ | | | | | | |
| FCS_CKM.1 | | ✓ | | | | | |
| FCS_COP.1 | | ✓ | | | | | |
| FDP_ACC.1 | | | | | | ✓ | |
| FDP_ACF.1 | | | | | | ✓ | |
| FIA_AFL.1 | | | | ✓ | ✓ | ✓ | |
| FIA_ATD.1 | | | | | | ✓ | |
| FIA_SOS.1 | | | | | ✓ | ✓ | |
| FIA_UAU.1 | | | | ✓ | ✓ | ✓ | |
| FIA_UAU.7 | | | | ✓ | ✓ | ✓ | |
| FIA_UID.2 | | | | ✓ | ✓ | ✓ | |
| FIA_USB.1 | | | | | | ✓ | |
| FMT_MOF.1 | | | | ✓ | | | |
| FMT_MSA.1 | | | | | | ✓ | |
| FMT_MSA.3 | | | | | | ✓ | |
| FMT_MTD.1 | | | | ✓ | | ✓ | |
| FMT_SMF.1 | | | | ✓ | | | |
| FMT_SMR.1 | | | | ✓ | | ✓ | |
| FPT_STM.1 | ✓ | | | | | | |

| Security Objectives | | | | | | | |
|----------------------------------|----------|----------|------------|----------|------------|--------|----------|
| Security Functional Requirements | O.AUDITS | O.CIPHER | O.COMM_SEC | O.MANAGE | O.RESTRICT | O.USER | O.VERIFY |
| FPT_TST.1 | | | | | | | ✓ |
| FTP_ITC.1 | | | ✓ | | | | |

Table 22: Security Objectives to SFR Rationale

| Security Objectives | Security Functional Requirements Rationale |
|---------------------|--|
| O.AUDITS | <p>O. AUDITS is the objective that provides the function to record auditable events and its log data.</p> <p>By satisfying the following security requirements, O.AUDITS can be realized.</p> <p>By FAU_GEN.1, the security audit log data are generated for the auditable events: (However, audit is unnecessary for the following functional requirements for each reason described below.)</p> <ul style="list-style-type: none"> - FAU_STG.4: The total number of security audit log data events is fixed. The data are stored and updated automatically. - FCS_CKM.1: When cryptographic key generation fails, a system error occurs at the time of booting of the MFD. - FCS_COP.1: An encryption failure is monitored as job status. - FMT_MSA.3: No change is to be applied to default values and rules. <p>By FAU_SAR.1, the authorized system administrator can read the security audit log data from an audit log file.</p> <p>By FAU_SAR.2, only the authorized system administrator can access the security audit log data.</p> <p>By FAU_STG.1, the security audit log data stored in an audit log file is protected from unauthorized deletion and alteration.</p> <p>By FAU_STG.4, when the security audit log data is full, the oldest stored audit record is overwritten and a new audit event is stored into the audit log file.</p> <p>By FPT_STM.1, the auditable events are recorded with time stamp in the audit log, using highly reliable clock of the TOE.</p> |
| O.CIPHER | <p>O. CIPHER is the objective that encrypts the used document data and the security audit log data in the eMMC memory so that they cannot be analyzed even if retrieved without authorization.</p> <p>By satisfying the following security requirements, O.CIPHER can be</p> |

| Security Objectives | Security Functional Requirements Rationale |
|---------------------|--|
| | <p>realized.</p> <p>By FCS_CKM.1, the cryptographic key is generated in accordance with the specified cryptographic key size (256 bits).</p> <p>By FCS_COP.1, the document data and security audit log data to be stored into the eMMC memory are encrypted and then decrypted when the data are read, in accordance with the determined cryptographic algorithm and cryptographic key size.</p> |
| O.COMM_SEC | <p>O.COMM_SEC is the objective that protects the document data, security audit log data, and TOE setting data on the internal network from interception and alteration.</p> <p>By satisfying the following security requirements, O.COMM_SEC can be realized:</p> <p>By FTP_ITC.1, a highly reliable communication channel is provided through communication data encryption protocol so that the document data, security audit log data, and TOE setting data on the internal network between the TOE and the IT product can be protected from threats.</p> |
| O.MANAGE | <p>O. MANAGE is the objective that allows only an authenticated system administrator to access the system administrator mode for security function setting and inhibits a general user from accessing the TOE setting data. By satisfying the following security requirements, O.MANAGE can be realized:</p> <p>In order to prevent attackers from using privileges given to system administrators and accessing protected assets, the power needs to be cycled in cases when the number of the key operator authentication failures by By FIA_AFL.1 (1), because the power needs to be cycled when the number of key operator authentication failures reaches the defined number of times.</p> <p>By FIA_AFL.1 (2), successive attacks are prevented because the power needs to be cycled when the number of SA authentication failures (at local authentication) reaches the defined number of times.</p> <p>By FIA_UAU.1 and FIA_UID.2, user authentication is performed to identify an authorized system administrator or general user.</p> <p>By FIA_UAU.7, unauthorized disclosure of the authentication information (password) is prevented because the authentication feedback is protected.</p> <p>By FMT_MOF.1, the person who enables/disables TOE security functions and makes functional settings is limited to system administrator.</p> <p>By FMT_MTD.1, the person who can make settings of TOE security</p> |

| Security Objectives | Security Functional Requirements Rationale |
|---------------------|---|
| | <p>functions is limited to system administrator. Thus, only system administrators can query, modify, and create TSF data.</p> <p>By FMT_SMF.1, TOE security management functions are provided for system administrator.</p> <p>By FMT_SMR.1 (1), the role related to the security is limited to system administrator by maintaining the role of system administrator as a user who has special authority.</p> |
| O.RESTRICT | <p>O.RESTRICT is the objective that offers the function to inhibit an unauthorized person from using the TOE.</p> <p>By satisfying the following security requirements, O.RESTRICT can be realized:</p> <p>In order to prevent attackers from using privileges given to system administrators and accessing protected assets, the power needs to be cycled in cases when the number of the key operator authentication failures by By FIA_AFL.1 (1), because the power needs to be cycled when the number of key operator authentication failures reaches the defined number of times.</p> <p>By FIA_AFL.1 (2), successive attacks are prevented because the power needs to be cycled when the number of SA authentication failures (at local authentication) reaches the defined number of times.</p> <p>By FIA_UIA.1 and FIA_UID.2, user authentication is performed to identify an authorized general user and system administrator.</p> <p>By FIA_UAU.7, unauthorized disclosure of the authentication information (password) is prevented because the authentication feedback is protected.</p> <p>By FIA_SOS1, the minimum length of password for SA and general user is limited.</p> |
| O.USER | <p>O.USER is the objective that identifies the TOE user and allows only the authorized user to retrieve, and delete the document data and to change password.</p> <p>By satisfying the following security requirements, O.USER can be realized:</p> <p>By FDP_ACC.1 and FDP_ACF.1, user authentication is performed. Only authorized user is allowed to operate the objects.</p> <p>In order to prevent attackers from using privileges given to system administrators and accessing protected assets, the power needs to be cycled in cases when the number of the key operator authentication failures by By FIA_AFL.1 (1), because the power needs to be cycled when the number of key operator authentication failures reaches the defined number of times.</p> |

| Security Objectives | Security Functional Requirements Rationale |
|---------------------|--|
| | <p>By FIA_AFL.1 (2), successive attacks are prevented because the power needs to be cycled when the number of SA authentication failures (at local authentication) reaches the defined number of times.</p> <p>By FIA_ATD.1 and FIA_USB.1, each role of key operator, SA, and general user is maintained and only the authorized users are associated with the subjects.</p> <p>By FIA_SOS1, the minimum length of password for user is limited.</p> <p>By FIA_UAU.1 and FIA_UID.2, user authentication is performed to identify an authorized general user and system administrator.</p> <p>By FIA_UAU.7, unauthorized disclosure of the authentication information (password) is prevented because the authentication feedback is protected.</p> <p>By FMT_MSA.1, the query, modify, deletion, and creation of security attributes are managed.</p> <p>By FMT_MSA.3, the suitable default values are managed.</p> <p>By FMT_MTD.1, the setting of password for key operator is limited to key operator, that for SA is limited to key operator and SA, and that for general user is limited to system administrator and the general user (when it is his/her own).</p> <p>By FMT_SMF.1, TOE security management functions are provided for authorized users.</p> <p>By FMT_SMR.1, the role of general user and system administrator is maintained and associated with the general user and system administrator.</p> |
| O. VERIFY | <p>O. VERIFY is the objective that provides the function to verify the integrity of TSF executable code.</p> <p>By satisfying the following security requirements, O. VERIFY can be realized.</p> <p>By FPT_TST.1 the TOE can execute the self test function to verify the integrity of TSF executable code and TSF data upon initiation.</p> |

6.3.2. Dependencies of Security Functional Requirements

Table 23 describes the functional requirements that security functional requirements depend

on and those that do not and the reason why it is not problematic even if dependencies are not satisfied.

Table 23: Dependencies of Functional Security Requirements

| Functional Requirement | Dependencies of Functional Requirements | |
|--|---|---|
| Requirement and its name | Requirement that is dependent on | Requirement that is not dependent on and its rationale |
| FAU_GEN.1 Audit data generation | FPT_STM.1 | - |
| FAU_SAR.1 Audit review | FAU_GEN.1 | - |
| FAU_SAR.2 Restricted audit review | FAU_SAR.1 | - |
| FAU_STG.1 Protected audit trail storage | FAU_GEN.1 | - |
| FAU_STG.4 Prevention of audit data loss | FAU_STG.1 | - |
| FCS_CKM.1 Cryptographic key generation (The stored data in the Flash memory) | FCS_COP.1 | FCS_CKM.4: As specified in the Organizational Security Policies, a cryptographic key does not need to be destructed. |
| FCS_COP.1 Cryptographic operation (The stored data in the Flash memory) | FCS_CKM.1 | FCS_CKM.4: As specified in the Organizational Security Policies, a cryptographic key does not need to be destructed. |
| FDP_ACC.1 Subset access control | FDP_ACF.1 | - |
| FDP_ACF.1 Security attribute based access control | FDP_ACC.1 FMT_MSA.3 | - |
| FIA_AFL.1 Authentication failure handling | FIA_UAU.1 | - |
| FIA_ATD.1 User attribute definition | None | |

| Functional Requirement | Dependencies of Functional Requirements | |
|--|---|--|
| Requirement and its name | Requirement that is dependent on | Requirement that is not dependent on and its rationale |
| FIA_SOS.1 Verification of secrets | None | |
| FIA_UAU.1 Timing of authentication | | FIA_UID.1: The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1. |
| FIA_UAU.7 Protected authentication feedback | | FIA_UAU.1: The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1. |
| FIA_UID.2 User identification before any action | None | |
| FIA_USB.1 User-subject binding | FIA_ATD.1 | - |
| FMT_MOF.1 Management of security functions behavior | FMT_SMF.1 FMT_SMR.1 | - |
| FMT_MSA.1 Management of security attributes | FDP_ACC.1 FMT_SMF.1 FMT_SMR.1 | - |
| FMT_MSA.3 Static attribute initialization | FMT_MSA.1 FMT_SMR.1 | - |
| FMT_MTD.1 Management of TSF data | FMT_SMF.1 FMT_SMR.1 | - |
| FMT_SMF.1 Specification of management functions | None | |
| FMT_SMR.1 Security roles | | FIA_UID.1: The dependency on FIA_UID.1 is satisfied because FIA_UID.2 is the functional security requirement that is an upper hierarchy of FIA_UID.1. |

| Functional Requirement | Dependencies of Functional Requirements | |
|--|---|--|
| Requirement and its name | Requirement that is dependent on | Requirement that is not dependent on and its rationale |
| FPT_STM.1 Reliable time stamp | | None |
| FPT_TST.1 TSF testing | | None |
| FTP_ITC.1 Inter-TSF Trusted Channel | | None |

6.3.3. Security Assurance Requirements Rationale

This TOE is for a MFD, a commercial product. The following threats are assumed to be caused by a low-level attacker: attack or interception/alteration of data on internal network via a MFD external interface from control panel, Web browser of system administrator's client; and reading-out of information by removing the eMMC memory and connecting it to a commercial tool.

To counter these threats, this TOE is required to provide the security functions which assure security.

ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7. TOE SUMMARY SPECIFICATION

This chapter describes the summary specifications of the security functions provided by this TOE.

7.1. Security Functions

Table 24 shows security functional requirements and the corresponding TOE security functions.

The security functions described in this section satisfy the TOE security functional requirements that are specified in section 6.1 of this ST.

Table 24: Security Functional Requirements and the Corresponding TOE Security Functions

| Security Functions Security Functional Requirements | TSF_CIPHER | TSF_USER_AUTH | TSF_FMT | TSF_CE_LIMIT | TSF_FAU | TSF_NET_PROT | TSF_SELF_TEST |
|--|------------|---------------|---------|--------------|---------|--------------|---------------|
| FAU_GEN.1 | | | | | ✓ | | |
| FAU_SAR.1 | | | | | ✓ | | |
| FAU_SAR.2 | | | | | ✓ | | |
| FAU_STG.1 | | | | | ✓ | | |
| FAU_STG.4 | | | | | ✓ | | |
| FCS_CKM.1 | ✓ | | | | | | |
| FCS_COP.1 | ✓ | | | | | | |
| FDP_ACC.1 | | ✓ | | | | | |
| FDP_ACF.1 | | ✓ | | | | | |
| FIA_AFL.1 (1) | | ✓ | | | | | |
| FIA_AFL.1 (2) | | ✓ | | | | | |
| FIA_ATD.1 | | ✓ | | | | | |
| FIA_SOS.1 | | ✓ | | | | | |
| FIA_UAU.1 | | ✓ | | | | | |
| FIA_UAU.7 | | ✓ | | | | | |
| FIA_UID.2 | | ✓ | | | | | |
| FIA_USB.1 | | ✓ | | | | | |
| FMT_MOF.1 | | | ✓ | ✓ | | | |
| FMT_MSA.1 | | ✓ | ✓ | | | | |
| FMT_MSA.3 | | | ✓ | | | | |
| FMT_MTD.1 | | ✓ | ✓ | ✓ | | | |
| FMT_SMF.1 | | ✓ | ✓ | ✓ | | | |

| Security Functions Security Functional Requirements | TSF_CIPHER | TSF_USER_AUTH | TSF_FMT | TSF_CE_LIMIT | TSF_FAU | TSF_NET_PROT | TSF_SELF_TEST |
|--|------------|---------------|---------|--------------|---------|--------------|---------------|
| FMT_SMR.1 | | ✓ | ✓ | ✓ | | | |
| FPT_STM.1 | | | | | ✓ | | |
| FPT_TST.1 | | | | | | | ✓ |
| FTP_TRP.1 | | | | | | ✓ | |

The summary of each TOE security function and the corresponding security functional requirements are described below.

7.1.1. Flash Memory Data Encryption (TSF_CIPHER)

The document data and security audit log data are encrypted before stored into the eMMC memory when operating any function of copy, print, Network Scan, or configuring various security function settings.

(1) FCS_CKM.1 Cryptographic key generation

The TOE generates a 256-bit encryption key with SHA-2 algorithm based on FIPS PUB 180-2.

(2) FCS_COP.1 Cryptographic operation

Before storing the document data and security audit log data into the eMMC memory, the TOE encrypts the data using the 256-bit cryptographic key and the AES algorithm based on FIPS PUBS 197. When reading out the stored data, the TOE decrypts the data also using the 256-bit cryptographic key and the AES algorithm.

7.1.2. User Authentication (TSF_USER_AUTH)

Access to the TOE functions is restricted to the authorized user.

A user needs to enter his/her ID and password from Web browser of the user client, or MFD control panel. After a user enters his/her ID and password, an MFD identifies and authenticates the user based on user information stored in the MFD or an external server.

There are the following two types of authentication depending on how user information is registered.

a) Local Authentication

In local authentication, authentication is managed by using the user information registered in the TOE.

b) Remote Authentication

Authentication is performed by remote authentication server. User information is not registered in the TOE. In remote authentication, authentication is performed by using the user information managed by remote authentication server (LDAP server or Kerberos server).

Only the authenticated user can use the following functions:

a) Functions controlled by the MFD control panel

Copy, network scan, and print (This print function requires the Store Print preset from printer driver. A user must be authenticated from the control panel for print job.)

b) Functions controlled by Embedded Web Server

Display of device condition, display of job status and its log.

In addition, access to and setting change of the TOE security functions are restricted to the authorized system administrator. A system administrator needs to enter his/her ID and password from MFD control panel or system administrator client.

(1) FIA_AFL.1 (1), FIA_AFL.1 (2) Authentication failure handling

The function of the authentication failures is provided for the System Administrator authentication which is performed before accessing the TOE. After the number of unsuccessful authentication attempts with a system administrator ID reaches 5 time upon local authentication, the system administrator with the said ID will not be authenticated until the TOE is powered off/on.

(2) FIA_ATD.1 User attribute definition

The function of the TOE to define and retain the roles of System Administrator and general user.

(3) FIA_SOS.1 Verification of secrets

When setting a password of System Administrator and general user, the TOE rejects settings if the password is less than the minimum number of characters.

(4) FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

The TOE requests a user to enter his/her ID and password before permitting him/her to operate the MFD function via Web browser of a user client, or the control panel. The entered user ID and password are verified against the data registered in the TOE setting data. This identification (FIA_UID.2) and the authentication (FIA_UAU.1) are simultaneously performed, and the operation is allowed only when both of the identification and authentication succeed.

When a print job is received from a user client, the TOE identifies a registered user ID and

stores the job without authenticating the user.

(5) FIA_UAU.7 Protected authentication feedback

The TOE offers the function to display the same number of asterisks (`*`) as the entered-password characters on the control panel, or Web browser, in order to hide the password at the time of user authentication.

(6) FIA_USB.1 User-subject binding

With the authenticated ID, TOE associates the roles of System Administrator, and general user with the subjects.

(7) FMT_MSA.1 Management of security attributes

With the user authentication function, the TOE permits the authenticated user to handle the security attributes as shown in Table 25.

Table 25: Management of security attributes

| Security Attributes | Operations | Roles |
|--|-----------------------|--------------------------------------|
| Key operator identifier | query | System Administrator |
| SA identifier (with local authentication only) | query, delete, create | System Administrator |
| General user identifier (with local authentication only) | query, delete, create | System Administrator |
| Store Print owner identifier | query, delete, create | System Administrator General user |

(8) FMT_MTD.1 Management of TSF data

FMT_SMF.1 Specification of management functions

The TOE provides the user interface for setting password only to the authenticated authorized user.

The setting of password for key operator is limited to key operator, that for SA (with local authentication only) is limited to key operator and SA, and that for general user (with local authentication only) is limited to system administrator and the general user (when it is his/her own).

(9) FMT_SMR.1 Security role

The TOE maintains the roles of system administrator and general user and associates these roles to the authorized users.

(10) FDP_ACC.1 Subset access control

FDP_ACF.1 Security attribute based access control

With the user authentication function, the TOE permits the authenticated user to operate Store Print as shown in Table 26.

Table 26: Access Control

| | Store Print |
|---------------------------|--|
| Creation of box | - |
| Deletion of box | - |
| Print of document data | Available for general user, System Administrator |
| Deletion of document data | Available for general user, System Administrator |

User authentication is performed before accessing Store Print.

a) Store Print Function

A user sends a print request from the printer driver in which the Store Print is preset, the print data are decomposed into bitmap data, classified according to the user ID, and temporarily stored in the eMMC memory.

To refer to the stored print data, a user needs to enter his/her ID and password from the control panel. When the user is authenticated, the data on the waiting list corresponding to the user ID are displayed. The user can request printing or deletion of the data on the list.

- Store Print Operation by a General User / System Administrator

When the general user identifier / SA identifier matches the owner identifier of Store Print area, print and deletion of the document data inside are allowed.

When the document data are deleted, the corresponding Store Print area is also deleted.

7.1.3. System Administrator's Security Management (TSF_FMT)

To grant a privilege to a specific user, this function allows only the authorized system administrator to access the system administrator mode which enables him/her to refer to and configure the settings of the following TOE security functions from the control panel or system administrator client.

(1) FMT_MOF.1 Management of security functions behavior

FMT_MTD.1 Management of TSF data

FMT_SMF.1 Specification of management functions

The TOE provides a user interface which allows only the authenticated system administrator to refer to / change the TOE setting data related to the following TOE security functions and to make setting whether to enable/disable each function.

With these functions, the required security management functions are provided.

The settings of the following TOE security functions can be referred to and changed from the control panel.

- Refer to the setting of TLS communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to and set date and time;

With Embedded Web Server, the settings of the following TOE security functions can be referred to and changed from a system administrator client via Web browser.

- Setting of the key operator password (only a key operator is privileged);
- Refer to the setting of ID of SA and general user and change the password (with local authentication only);
- Refer to the setting of access denial due to authentication failures of system administrator, enable/disable it, and set the allowable number of the failures before access denial;
- Refer to and set date and time;
- Refer to and set Self Test;
- Refer to and set the minimum password length (with local authentication only);
- Refer to the setting of Security Audit Log and enable/disable it, (When Security Audit Log data are enabled, security audit log data can be downloaded in the form of tab-delimited text to a system administrator client.);
- Refer to the setting of TLS communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of IPSec communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Refer to the setting of S/MIME communication of Internal Network Data Protection, enable/disable it, and configure the details;
- Download/upload and create an X.509 certificate;
- Refer to the setting of User Authentication and select disable/Local Authentication/Remote Authentication, and configure the details;
- Refer to and set general user permission;
- Refer to and set Customer Engineer Operation Restriction;

(2) FMT_MSA.1 Management of security attributes

The TOE restricts the handling of the general user identifier only to a system administrator.

(3) FMT_MSA.3 Static attribute initialization

Regarding Store Print, the TOE sets the user identifier created as owner identifier and the available user identifier, and set them as default values of security attributes.

(4) FMT_SMR.1 Security roles

The system administrator's role is maintained and the role is associated with a system administrator.

7.1.4. Customer Engineer Operation Restriction (TSF_CE_LIMIT)

A system administrator can restrict CE's operation in the system administrator mode to inhibit CE from referring to / changing the settings related to System Administrator's Security Management (TSF_FMT). This function can prevent setting change by an attacker who is impersonating CE.

(1) FMT_MOF.1 Management of security functions behavior

FMT_MTD.1 Management of TSF data

FMT_SMF.1 Specification of management functions

The TOE provides a user interface which allows only the authenticated system administrator to refer to / change (enable/disable) the TOE settings related to Customer Engineer Operation Restriction from the Embedded Web Server.

With these functions, the required security management functions are provided.

(2) FMT_SMR.1 Security roles

The system administrator's role is maintained and the role is associated with a system administrator.

7.1.5. Security Audit Log (TSF_FAU)

According to Security Audit Log setting which is configured by a system administrator using the system administrator mode, the important events of the TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function. All the TOE users are the targets of this audit log.

(1) FAU_GEN.1 Audit data generation

It is assured that the defined auditable event is recorded in the audit log.

Table 27 shows the details of the audit log data.

Table 27: Details of Security Audit Log Data

The auditable events are recorded with the following fixed size entries:

- Log ID: consecutive numbers as an audit log identifier (1 - 60000)
- Date: date data (yyyy/mm/dd, mm/dd/yyyy, or dd/mm/yyyy)
- Time: time data (hh:mm:ss)
- Logged Events: event name (arbitrary characters of up to 32 digits)
- User Name: user name (arbitrary characters of up to 32 digits)
- Description: description on events
(arbitrary characters of up to 32 digits, see below for details)
- Status: status or result of event processing
(arbitrary characters of up to 32 digits, see below for details)
- Optionally Logged Items: additional information recorded to audit log
(except common record items)

| Logged Events | Description | Status |
|---------------------------------|--|--|
| Change in Device Status | | |
| System Status | Started normally (cold boot) | - |
| | Started normally (warm boot) | |
| | Shutdown requested | |
| | User operation (Local) | Start/End |
| | Self Test | Successful/Failed |
| User Authentication | | |
| Login/Logout | Login | Successful, Failed (Invalid UserID), Failed (Invalid Password), Failed |
| | Logout | |
| | Locked System Administrator Authentication | - (Number of authentication failures recorded) |
| | Detected continuous Authentication Fail | |
| Change in Audit Policy | | |
| Audit Policy | Audit Log | Enable/Disable |
| Job Status | | |
| Job Status | Print | Completed, Completed with Warnings, Canceled by User, Canceled by Shutdown, Aborted, Unknown |
| | Copy | |
| | Scan | |
| | Print Reports | |
| Change in Device Settings | | |
| Device Settings | Adjust Time | Successful/Failed |
| | Switch Authentication Mode | Successful |
| | Change Security Setting | (Setting items recorded) |
| Access to Data Stored in Device | | |
| Device Data | Import Certificate | Successful/Failed |

| Logged Events | Description | Status |
|----------------------|-----------------------|---|
| | Delete Certificate | |
| | Add Address Entry | |
| | Delete Address Entry | |
| | Edit Address Entry | |
| | Export Audit Log | |
| Communication Result | | |
| Communication | Trusted Communication | Failed (Protocol and communication destination stored) |

(2) FAU_SAR.1 Audit review

It is assured that all the information recorded in the audit log can be retrieved.

Security audit log data can be downloaded in the form of tab-delimited text by pressing the button “store as a text file.” To download security audit log data, TLS communication needs to be enabled before using Web browser.

(3) FAU_SAR.2 Restricted audit review

The person who retrieves the security audit log data is limited to the authenticated system administrator. A system administrator can access the security audit log data only via Web browser and the access from the control panel is inhibited. Therefore, a system administrator needs to log in from Web browser to access the security audit log data.

(4) FAU_STG.1 Protected audit trail storage

There is no function to delete the security audit log data, and the security audit log data are protected from untrusted alteration and modification.

(5) FAU_STG.4 Prevention of audit data loss

When security audit log data are full, the oldest stored audit record is overwritten with the new data so that the new data is not lost but surely recorded.

Auditable events are stored with time stamps into NVRAM. When the number of stored events reaches 50, the 50 logs on NVRAM is stored into one file (“audit log file”) within the eMMC memory. Up to 15,000 events can be stored. When the number of recorded events exceeds 15,000, the oldest audit log file is overwritten and a new audit event is stored.

(6) FPT_STM.1 Reliable time stamps

The time stamp of TOE’s clock function is issued when the defined auditable event is recorded in the audit log file.

By TSF_FMT, only a system administrator is enabled to change the clock setting.

7.1.6. Internal Network Data Protection (TSF_NET_PROT)

Internal Network Data Protection is provided by the following four protocols which are configured by a system administrator using the system administrator mode:

(1) FTP_ITC.1 Inter-TSF Trusted Channel

The document data, security audit log data, and TOE setting data are protected by the encryption communication protocol that ensures secure data communication between the TOE and the IT products. This trusted channel is logically distinct from other communication channel and provides assured identification of its endpoints and protection of the communication data from modification or disclosure.

The followings are the encryption algorithms for network communication provided by the TOE.

| Protocol | Target Products. | Encryption Algorithms |
|----------|---|--|
| TLS | Client PC (Web Browser, Printer Driver) LDAP Server | AES/128 bits AES/256 bits |
| IPSec | Client PC (Web Browser, Printer Driver) LDAP Server Kerberos Server SMTP Server FTP Server DNS Server | AES/128 bits Triple-DES/168 bits |
| S/MIME | SMTP Server | Triple-DES/168 bits AES/128 bits AES/192 bits AES/256 bits |

a) TLS

According to the TLS communication which is configured by a system administrator using the system administrator mode, TLS ensuring secure data transmission is supported. This protects the security of document data, security audit log data, and TOE setting data on the internal network.

By supporting TLS, the TOE can act as TLS server or TLS client. Moreover, TLS can protect data transmission between the TOE and the remote from interception and alteration. Protection from interception is realized by encrypting transmission data with the following cryptographic keys. A cryptographic key is generated at the time of starting a session and lost at the time of ending the session or powering off the MFD main unit.

Cryptographic key generated as TLSv1.0/TLSv1.1/TLSv1.2 upon every session

Specifically, one of the cryptographic suites below is adopted:

| Cryptographic Suites of TLS | Cryptographic Method and Size of Secret Key | Hash Method |
|---------------------------------|---|-------------|
| TLS_RSA_WITH_AES_128_CBC_SHA | AES / 128 bits | SHA-1 |
| TLS_RSA_WITH_AES_256_CBC_SHA | AES / 256 bits | SHA-1 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 | AES / 128 bits | SHA256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | AES / 256 bits | SHA256 |

Protection from the alteration is realized by HMAC (Hashed Message Authentication Code - IETF RFC 2104) of TLS.

When TLS communication is enabled on the Web client, requests from the client must be received via HTTPS. The TLS communication needs to be enabled before IPSec or S/MIME is enabled or before security audit log data are downloaded by a system administrator.

b) IPSec

According to the IPSec communication which is configured by a system administrator using the system administrator mode, IPSec ensuring secure data transmission is supported. This protects the security of document data, security audit log data, and TOE setting data on the internal network.

IPSec establishes the security association to determine the parameters (e.g. private key and cryptographic algorithm) to be used in the IPSec communication between the TOE and the remote. After the association is established, all transmission data among the specified IP addresses are encrypted by the transport mode of IPSec until the TOE is powered off or reset. A cryptographic key is generated at the time of starting a session and lost at the time of ending the session or powering off the MFD main unit.

Cryptographic key generated as IPSec (ESP: Encapsulating Security Payload) at every session. Specifically, one of the following combinations between secret-key cryptographic method and hash method is adopted:

| Cryptographic Method and Size of Secret Key | Hash Method |
|---|-------------------------------|
| AES / 128 bits | SHA-1, SHA256, SHA384, SHA512 |
| 3-Key Triple-DES / 168 bits | SHA-1, SHA256, SHA384, SHA512 |

c) S/MIME

According to the S/MIME communication which is configured by a system administrator using the system administrator mode, S/MIME ensuring secure mail communication is supported. This protects the security of document data on the internal and external networks.

By S/MIME encrypting mail function, the document data being transmitted to the outside by E-mail are protected from interception.

A cryptographic key is generated at the time of starting mail encryption and lost at the time of completion of the encryption or powering off the MFD main unit.

Secret-key cryptographic method generated as S/MIME for every mail

| Cryptographic Method and Size of Secret Key |
|---|
| 3Key Triple-DES/168 bits |
| AES / 128 bits |
| AES / 192 bits |
| AES / 256 bits |

7.1.7. Self Test (TSF_S_TEST)

The TOE can execute a self test function to verify the integrity of TSF executable code and TSF data.

(1) FPT_TST.1 TSF testing

TOE verifies the area of NVRAM and EEPROM including TSF data upon initiation, and displays an error on the control panel if an error occurs.

However, an error is not detected for the data on audit logs and time and date as these are not included in the target. Also, when Self Test function is set to be executed upon initiation, TOE calculates the checksum of Controller ROM to confirm if it matches the specified value, and displays an error on the control panel if an error occurs.

8. ACRONYMS AND TERMINOLOGY

8.1. Acronyms

The following acronyms are used in this ST:

| Acronym | Definition |
|----------|--|
| ADF | Auto Document Feeder |
| CC | Common Criteria |
| CE | Customer Engineer / Customer Service Engineer |
| DRAM | Dynamic Random Access Memory |
| EAL | Evaluation Assurance Level |
| eMMC | Embedded Multi-Media Card |
| FIPS PUB | Federal Information Processing Standard publication |
| IIT | Image Input Terminal |
| IOT | Image Output Terminal |
| IT | Information Technology |
| IP | Internet Protocol |
| MFD | Multi-Function Device |
| NVRAM | Non Volatile Random Access Memory |
| PDL | Page Description Language |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| EEPROM | Serial Electronically Erasable and Programmable Read Only Memory |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SMTP | Simple Mail Transfer Protocol |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |

8.2. Terminology

The following terms are used in this ST:

| Term | Definition |
|-------------------------------------|---|
| User | Any entity outside the TOE who interacts with the TOE: <i>i.e.</i> general user, system administrator. |
| System Administrator Privilege (SA) | A user authorized by key operator to manage MFD maintenance and configure TOE security functions. |
| System Administrator | An authorized user who manages MFD maintenance and configures TOE security functions. This term covers both key operator and SA. |
| Customer Engineer (CE) | Customer service engineer, an engineer who maintains and repairs MFD. |
| Attacker | A malicious user of TOE |
| Control Panel | A panel of MFD on which buttons, lamps, and a touch screen panel are mounted to operate the MFD |
| General User Client | A client for general user. |
| System Administrator Client | A client for system administrator. An administrator can refer to and rewrite TOE setting data of MFD via Web browser. |
| Embedded Web Server | Embedded Web Server is a service on a Web server in the TOE to confirm the status of the TOE, change settings, job deletion of the TOE via the Web browser of the user client. Embedded Web Server can be used with the Windows standard Web browser. |
| System Administrator Mode | An operation mode that enables a system administrator to refer to and rewrite TOE setting for device operation and that for security functions according to the operational environment. This mode is distinguished from the operation mode that enables a general user to use the MFD functions. |
| Printer driver | Software to convert the data on a general user client into print data written in page description language (PDL), a readable format for MFD. Used on the user client. |
| Print Data | The data written in PDL, a readable format for MFD, which are to be converted into bitmap data by the TOE decompose function. |
| Control Data | The data that are transmitted by command and response interactions. This is one the type of the data transmitted between MFD hardware units. |
| Bitmap Data | The decomposed data of the data read by the copy function and the print data transmitted from a user client to MFD by the print function. Bitmap data are stored into the eMMC memory after being compressed |

| Term | Definition |
|---------------------------|--|
| | in the unique process. |
| Decompose Function | A function to analyze and convert the print data written in PDL into bitmap data. |
| Decompose | To analyze and convert the data written in PDL into bitmap data by the decompose function. |
| Original | Texts, images and photos to be read from IIT in the copy function. |
| Document Data | Document data means all the data, including images, transmitted across the MFD when any of copy, print, or network scan functions is used by a general user. The document data includes: - Bitmap data read from IIT and printed out from IOT (copy function), - Print data sent by general user client and its decomposed bitmap data (print function), |
| Used Document Data | The remaining data in the MFD eMMC memory even after deletion. The document data are first stored into the eMMC memory, used, and then only their files are deleted. |
| Security Audit Log Data | The chronologically recorded data of important events of the TOE. The events such as device failure, configuration change, and user operation are recorded based on when and who caused what event and its result. |
| Internally Stored Data | The data which are stored in a general user client or in the general client and server, but do not include data regarding TOE functions. |
| General Data | The data on the internal network. The general data do not include data regarding TOE functions. |
| TOE Setting Data | The data which are created by the TOE or for the TOE and may affect the TOE security functions. Included in the TSF data, specifically they include the information regarding the functions of System Administrator's Security Management, Customer Engineer Operation Restriction, ID and password of users, access denial due to authentication failure of system administrator, Internal Network Data Protection, Security Audit Log, User Authentication, User permission, Report Print, Auto Clear, Data/Time, and Self Test. |
| General Client and Server | Client and server which do not directly engage in TOE operations |
| Cryptographic Key | The 256-bit data which is automatically generated. Before the data are stored into the eMMC memory, they are encrypted with the cryptographic key. |
| Network | A general term to indicate both external and internal networks. |
| External Network | The network which cannot be managed by the organization that manages the TOE. This does not include the internal network. |
| Internal Network | Channels between MFD and highly reliable remote server / client PC. The channels are located in the network of the organization, the owner |

| Term | Definition |
|-----------------------|---|
| | of the TOE, and are protected from the security risks coming from the external network. |
| User Authentication | A function to limit the accessible TOE functions by identifying the user before he/she uses each TOE function. There are two modes, Local Authentication and Remote Authentication, and either mode is used for operation. |
| Local Authentication | A mode to manage user authentication of the TOE using the user information registered in the MFD. |
| Remote Authentication | A mode to manage user authentication of the TOE using the user information registered in the remote authentication server. |

9. REFERENCES

The following documentation was used to prepare this ST.

| Short Name | Document Title |
|-------------|---|
| [CC Part 1] | Part 1: Introduction and general model (September 2012 Version 3.1 Revision 4) Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 1: Introduction and general model, dated September 2012, CCMB-2012-09-001 (Japanese version 1.0, dated November 2012, translated by Information-Technology Promotion Agency, Japan) |
| [CC Part 2] | Part 2: Security functional components (September 2012 Version 3.1 Revision 4) Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 2: Security functional components, dated September 2012, CCMB-2012-09-002 (Japanese version 1.0, dated November 2012, translated by Information-Technology Promotion Agency, Japan) |
| [CC Part 3] | Part 3: Security assurance components (September 2012 Version 3.1 Revision 4) Common Criteria for Information Technology Security Evaluation - Version 3.1 Part 3: Security assurance components, dated September 2012, CCMB-2012-09-003 (Japanese version 1.0, dated November 2012, translated by Information-Technology Promotion Agency, Japan) |
| [CEM] | Common Methodology for Information Technology Security Evaluation - Version 3.1 Evaluation Methodology, dated September 2012, CCMB-2012-09-004 (Japanese version 1.0, dated November, translated by Information-Technology Promotion Agency, Japan) |