Security Card Type M19

DataOverwriteSecurity Unit Type M19

Security Target

Authors : RICOH COMPANY, LTD.
Date : 2016-02-24
Version : 3.03

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

Update History

Version	Date	Authors	Details
3.03	2016-2-24	RICOH COMPANY, LTD.	Released version

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This section describes the ST reference, TOE reference, TOE overview, and TOE description.

1.1 ST Reference

The following are the identification details of this ST.

Title	:	Security Card Type M19 DataOverwriteSecurity Unit Type M19 Security Target
Version	:	3.03
Date	:	2016-02-24
Authors	:	RICOH COMPANY, LTD.

1.2 TOE Reference

This TOE is Security Card Type M19 (Japanese name)/DataOverwriteSecurity Unit Type M19 (English name), which is manufactured by RICOH COMPANY, LTD. The TOE is identified by the following manufacturer, TOE names, and version. "Security Card Type M19" is the product name of this TOE when it is marketed in Japan, and "DataOverwriteSecurity Unit Type M19" when marketed in overseas countries. While the product names are different in Japanese and overseas markets, the software is identical.

Manufacturer: RICOH COMPANY, LTD.

TOE name: Security Card Type M19 (Japanese name)

DataOverwriteSecurity Unit Type M19 (English name)

Version: 1.02

1.3 TOE Overview

This section defines the TOE type, non-TOE hardware and software that are required for operations, TOE usages, and major TOE security functions.

1.3.1 TOE Type

The TOE is an optional software product for RICOH's digital Multi Function Product (hereafter "MFP"). The TOE utilises overwriting methods for data on the MFP's memory media.

Overwriting methods are used to prevent data retrieval by overwriting with specific values the data on the storage media.

1.3.2 Required Non-TOE Hardware and Software

This TOE is an optional software product for RICOH's MFP. This TOE is installed on the appropriate MFP products and used. Annex A shows the names of such MFP products. Standard hard disks in MFPs, on which this TOE can be installed, do not provide automatic encryption. Optional hard disks that provide automatic encryption cannot be used for this TOE.

MFP users can refer to the optional product list (product information that contains available optional products) created for each MFP product, to identify MFPs that the TOE can be installed on.

An MFP is an IT product that enables users to perform Copy, Print, Scan, Fax, and Document Server Functions.
When these functions are performed and the hard disk (hereafter "HDD") of the MFP is mounted, part or all of the document will be stored on the HDD as temporary working data. Deleting a document that was stored by using the MFP's Document Server Function is executed by logical deletion of data. The actual document data at this time remains on the HDD.

1.3.3 TOE Usage

The TOE is an optional product of the MFP and stored on an SD card, which will be distributed to users. In order to use the TOE, a customer engineer must install the TOE.
If the TOE is enabled, buttons and icons that are related to the TOE functions will be displayed on the MFP's Operation Panel. The Operation Panel allows users to configure TOE settings or select TOE functions for operations.

1.3.4 TOE Major Security Features

To erase data, the TOE applies data overwrite operations and invalidates data on the areas of the hard disk (hereafter "HDD") that the MFP specifies.

1.4 TOE Descriptions

This section defines physical scope of the TOE, user guidance documents, and logical scope of the TOE.

1.4.1 Physical Scope of TOE

The TOE is a loadable software product that runs on the MFP. In order to specify the physical scope of the TOE, the environment for MFP operations and TOE positioning in the operation environments will be specified.

1.4.1.1 MFP Operation Environment

It is assumed that the MFP will be installed in an office environment so that it can be connected to an internal or external network, telephone lines, or client computers through USB, corresponding to user needs. Once connected to a network, the MFP can communicate with client computers, FTP servers, SMB servers, or SMTP servers. If connected to a telephone line, the MFP can send and receive fax data. An assumed working environment of the MFP is outlined in Figure 1.

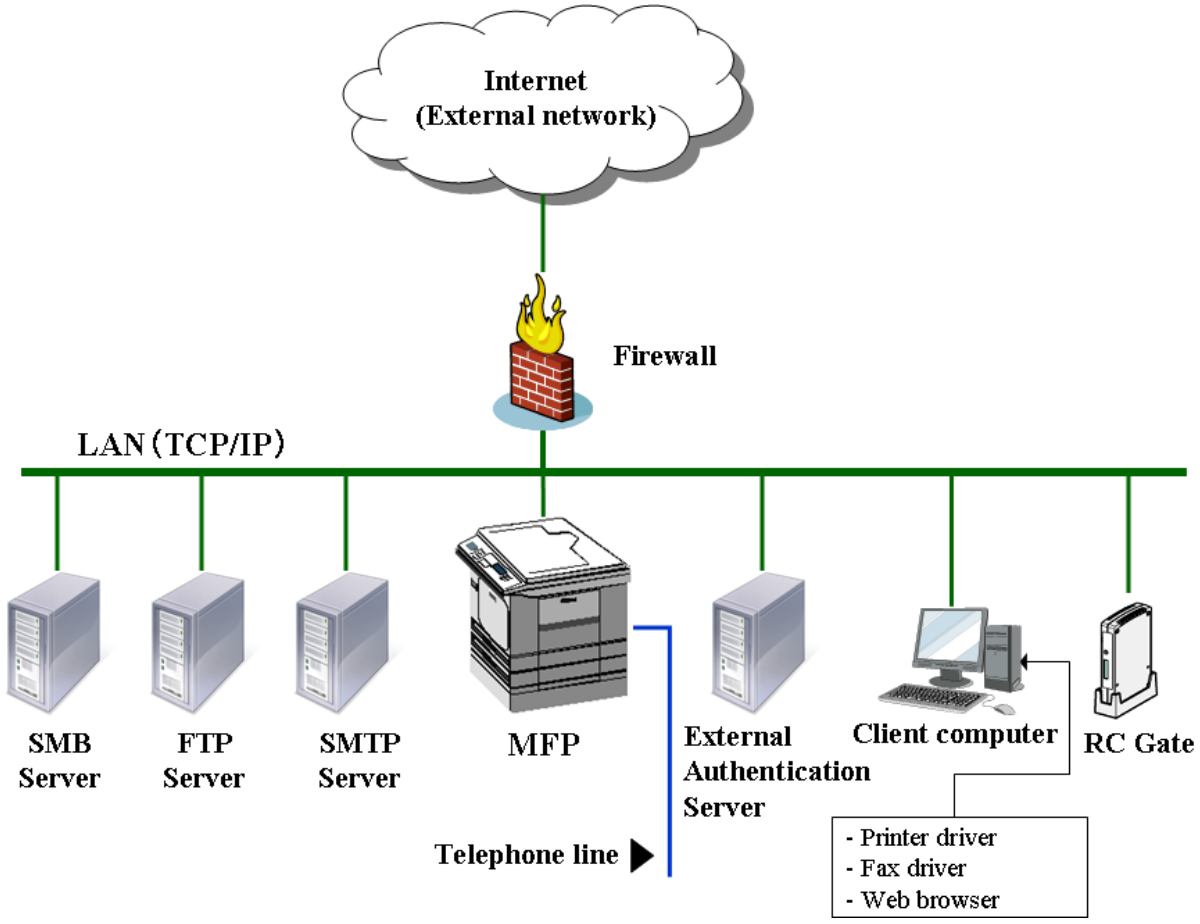


Figure 1: MFP Working Environment

1.4.1.2 TOE Positioning in MFP Operation Environment

The MFP's hardware configuration includes the following: an Operation Panel, an Engine Unit, a Fax Unit, a Controller Board, an HDD, a Network Unit, USB Ports, and an SD Card Slot. See Figure 2 below for the MFP's hardware configuration.

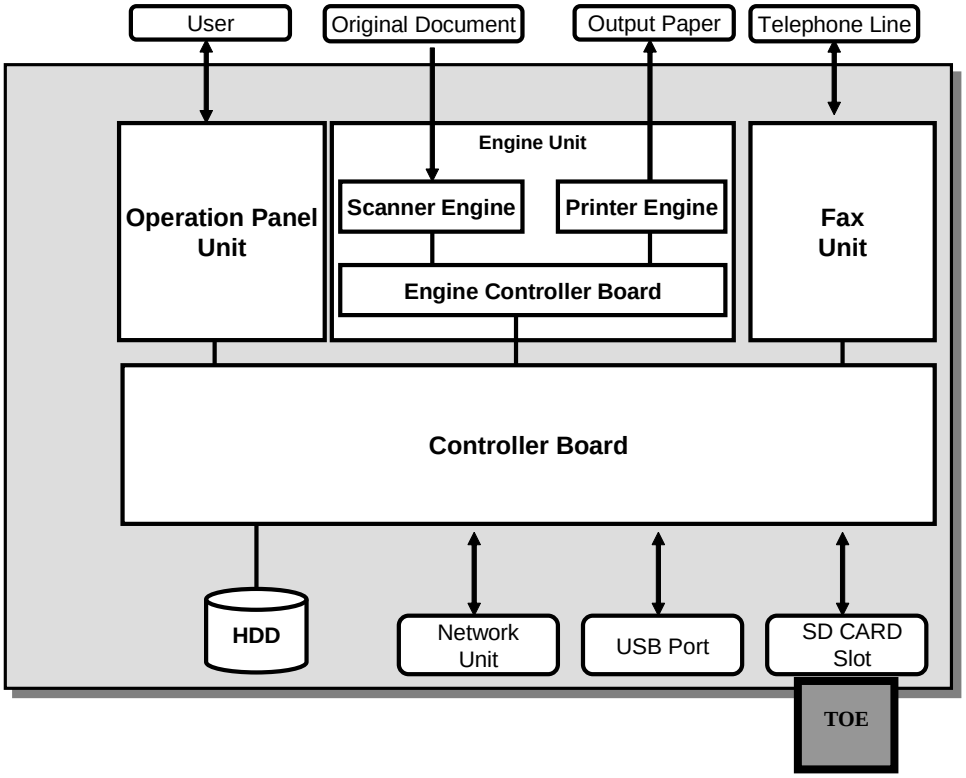


Figure 2: MFP's Hardware Configuration and TOE Positioning

The firmware to control MFP operations is installed in memory on the Controller Board. The SD card the TOE is stored in is inserted into the SD Card Slot of the MFP. The SD card is used to load the TOE on the MFP. Once loaded, the TOE communicates with the MFP's firmware and applies data overwrite operations to delete data that is stored on the HDD.

1.4.2 User Guidance Documents

Below are the user guidance documents that are provided for users when the TOE is supplied.

If the TOE is shipped to users in Japan, the user guidance documents in Japanese will be provided. If shipped to users in overseas countries, the user guidance documents in English will be provided. Because the user guidance in English is a translated version of the user guidance documents in Japanese, so the contents are the same in both Japanese and English.

- Name of Japanese guidance documents

  Security Card Type M19
  Operating Instructions D3BS-7000

- Name of English guidance documents

  DataOverwriteSecurity Unit Type M19
  Operating Instructions D3BS-7002

1.4.3 Logical Scope of TOE

The TOE functionality consists of sequential and batch overwriting. The Sequential and Batch Overwrite Functions are described below.
See "1.4.4 MFP Functions Related to the TOE" for the Auto Erase Memory Function and the Erase All Memory Function that are provided by MFP, which is outside the TOE.

Sequential Overwrite Function

The TOE will overwrite the specific data on the HDD area specified by the MFP. Users can select a data erasure method from NSA, DoD, and random number methods. All of these methods are within the TOE logical scope. (However, when the random number method is selected, data is overwritten one to nine times with random numbers.) When the Auto Erase Memory Function is applied and the unnecessary data area is identified on the HDD, the MFP specifies the HDD area that the data overwrite operations of the Sequential Overwrite Function is applied to.

Batch Overwrite Function

The TOE will delete all of the data, following the MFP instructions by overwriting the specific data on all areas of the HDD. Users can select a data erasure method from NSA, DoD, random number, BSI/VSITR, Secure Erase, and formatting methods. Only NSA, DoD, random number (in this case, data is overwritten one to nine times with random numbers), and BSI/VSITR methods are the ones within the TOE logical scope. When the user specifies the Batch Overwrite Function on the Operation Panel and this function is initiated, the MFP will send instructions for batch overwrite operations to the TOE.

1.4.4 MFP Functions Related to TOE

The Sequential and Batch Overwrite Functions of the TOE are hierarchical to the Auto Erase Memory Function and the Erase All Memory Function of the MFP. In addition, the Sequential and Batch Overwrite Functions are related to the following functions of the MFP: Residual Information Management Function, Sequential Overwrite Operation Configuration Function, Batch Overwrite Start-up/Suspension Function, and Residual Information Status Display Function. TOE functions and MFP functions related to the TOE are outlined in Figure 3, and each function is explained below:

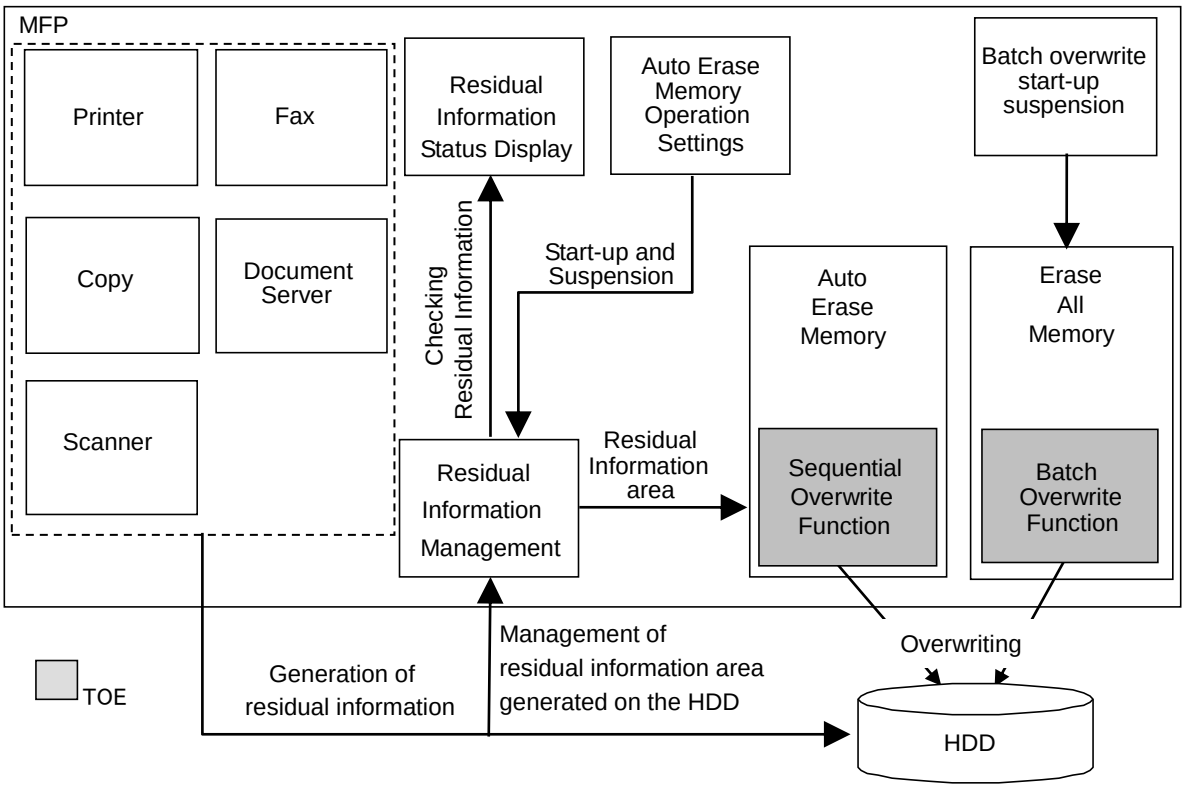


Figure 3: TOE Functions and MFP Functions Related to the TOE

Auto Erase Memory Function

A function to erase the following information on the HDD by using the Sequential Overwrite Function of the TOE.

- A piece of or all information of documents generated on the HDD when the MFP executes a document-related function

- Actual document data when a document is deleted by the Document Server Deletion Function. Because the Document Server Deletion Function logically deletes files, this function does not erase the actual document data.

Erase All Memory Function

A function to overwrite all areas on the HDD by using the Batch Overwrite Function of the TOE if users select the start-up of the function.

This function can be used to invalidate the document data or authorised MFP user information that is stored on the HDD of the MFP if the MFP is physically disposed of or transferred to another section.

Residual Information Management Function

A function to monitor whether information specified for the Auto Erase Memory Function is generated on the HDD, and when generated, to notify the Auto Erase Memory Function of the applicable area.

Auto Erase Memory Operation Setting Function

A function to enable or disable the Auto Erase Memory Function from the MFP's Operation Panel.
Only the MFP administrators are allowed to enable or disable the Auto Erase Memory Function.

Batch Overwrite Start-up/Suspension Function

A function to start or suspend the Erase All Memory Function from the MFP's Operation Panel. Only the MFP administrators are allowed to start or suspend the Erase All Memory Function.

Residual Information Status Display Function

A function to display three statuses, presence or absence of information specified for the Auto Erase Memory Function, or information being overwritten, on the MFP's Operation Panel.

2 Conformance Claims

This chapter describes CC conformance claims, PP conformance claims, conformance claims for security requirements package, and conformance claims rationale.

2.1 CC Conformance Claims

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

- CC version this ST and TOE claims conformance for:
  Part 1:
  Introduction and general model, September, 2012 Ver.3.1 Revision 4 [Japanese translated version 1.0] CCMB-2012-09-001
  Part 2:
  Security functional components, September, 2012 Ver.3.1 Revision 4 [Japanese translated version 1.0] CCMB-2012-09-002
  Part 3:
  Security assurance components, September, 2012 Ver.3.1 Revision 4 [Japanese translated version 1.0] CCMB-2012-09-003
- Functional requirements: Part 2 Extended
- Assurance requirements: Part 3 Conformant

2.2 PP Conformance Claims

This ST claims no conformance to PPs.

2.3 Conformance Claims for Security Requirement Packages

This ST claims conformance for the following security requirements:

- This ST claims no conformance for functional requirement packages.
- Assurance requirement packages are EAL2 conformant.

2.4 Conformance Claim Rationale

This ST claims no conformance to PPs, so the rationale for conformance claims is not relevant.

3 Security Problems

This section defines threats, organisational security policies, and assumptions.

3.1 Threats

No threats can be identified that the TOE and its operational environment counter.

3.2 Organisational Security Policies

This section identifies the organisational security policy that the TOE shall follow.

P.UNREADABLE

The TOE shall prevent the data in the area on the HDD that the MFP specifies from being read.

3.3 Assumptions

This section identifies assumptions that are related to the TOE environment.

A.MODE.AUTOMATIC

The TOE operations shall not be interrupted by MFP power-off before the TOE completes overwrite operations by the sequential overwriting method.

A.MODE.MANUAL

Against user's will, the implementation of the Batch Overwrite Function of the TOE shall not be unintentionally suspended by the operation of temporary suspension button or the MFP power-off, before the TOE completes overwrite operations by the Batch Overwrite Function.

A.MFP

The MFP with the TOE installed shall be properly set up and operated without any failure.

4 Security Objectives

This section defines the security objectives for the TOE and the TOE's operational environment

4.1 TOE Security Objectives

This section identifies the security objectives that can be applied to the TOE.

O.OVERWRITE

To eliminate any potential leakage of the data that is stored on the HDD area that the MFP specifies, the TOE applies overwrite operations to the area and invalidates the data.

4.2 Security Objectives for TOE's Operational Environment

This section identifies the security objectives for the TOE's operational environment.

OE.MODE.AUTOMATIC

When turning off the MFP, the user shall check the operational status of the icon on the Operation Panel. If the overwrite operations by the sequential overwrite method is complete, the user can turn off the machine.

OE.MODE.MANUAL

When applying the Batch Overwrite Function, the user shall ensure that the batch overwrite operations for the MFP will not be suspended unintentionally. The unintentional suspension means the operation of temporary suspension button or the MFP power-off.

OE.MFP.SETUP

The MFP for the TOE's operational environment shall be properly set up and operated so that the TOE can correctly function.

OE. MFP.NORMAL

If any failure occurs in the MFP for the TOE's operational environment, the MFP is controlled so that its operation stops.

4.3 Rationale for Security Objectives

The security objectives are designed to achieve the organisational security policies or satisfy the assumptions that are specified in "3 Security Problems". The relationship between the security objectives and the organisational security policies as well as assumptions is specified below in Table 1.

Table 1: Relationship between Security Objectives and Security Problems

Security problems / Security objectives	P.UNREADABLE	A.MODE.AUTOMATIC	A.MODE.MANUAL	A.MFP
O.OVERWRITE	X			
OE.MODE.AUTOMATIC		X		
OE.MODE.MANUAL			X	
OE.MFP.SETUP				X
OE.MFP.NORMAL				X

P.UNREADABLE

P.UNREADABLE is enforced by O.OVERWRITE because O.OVERWRITE ensures that data overwrite operations applied to the HDD area that the MFP specifies make the data in the area unreadable.

A.MODE.AUTOMATIC

A.MODE.AUTOMATIC is achieved by OE.MODE.AUTOMATIC because completion of the TOE's overwrite operations prior to the MFP's power loss ensures that the TOE's overwrite operations are not interrupted.

A.MODE.MANUAL

A.MODE.MANUAL is achieved by OE.MODE.MANUAL because the user management of the MFP during batch overwrite operations prevents the overwrite operations from being suspended unintentionally.

A.MFP

A.MFP is achieved by OE.MFP.SETUP and OE.MFP.NORMAL because the MFP for the TOE's operational environment is set up under the user management, and if any failure occurs in the MFP, its operation stops.

5 Extended Components Definition

This section defines the extended components of security function components and security assurance components.

5.1 Extended Components of Security Function Components

Directed by the following reasons, this ST defines FDP_SIP.1, which is an extended component of the security function components that are specified in the CC Part 2.

Rationale for necessity for component extension and component family augmentation

The TOE invalidates the data that is stored on the partial or entire area of the data resource a trusted IT product specifies, and the TSF does not control this data resource. FDP_RIP is a component family in the existing CC components that invalidates data. The data FDP_RIP invalidates is part of the data the TSF controls. This indicates that the data the TOE invalidates differs from the one FDP_RIP invalidates, so no refinement can be provided for FDP_RIP components (FDP_RIP.1.1, etc.).
Moreover, if new components are added to FDP_RIP, it may be wrongly conceived that the partial or entire data the TOE invalidates is stored in the data resource the TSF controls. For this, a new component family must be added. This new component family is defined as SIP.

Rationale for applicable class

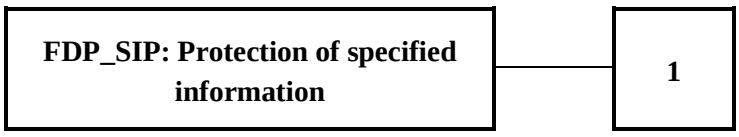
Generally, the data a trusted IT product specifies and the TOE applies overwrite operations to is the user data of the trusted IT product. For this, the appropriate class for extended components is FDP class.

FDP_SIP Protection of specified information

- Family behaviour

This family requires that any data in the data resource a trusted IT product specifies shall be invalid.

- Component levelling



FDP_SIP.1 requires that the TSF shall ensure no data in the specified data resource can be reused.

- Management: FDP_SIP.1

There are no management activities foreseen.

A trusted IT product manages all functions the TOE provides, and only the IT product can use the TOE functions. For this reason, no management activities are required.

- Audit: FDP_SIP.1

There are no auditable events foreseen.

FDP_SIP.1	**Protection of specified information**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SIP.1.1	The TSF shall ensure any data in the specified data resource is overwritten.

5.2 Extended Components of Security Assurance Components

No extensions augment the security assurance components.

6 Security Requirements

This section defines security functional requirements, security assurance requirements, and security requirements rationale.

6.1 Security Functional Requirements

This section demonstrates the security functional requirement the TOE provides.

FDP_SIP.1	**Protection of specified information**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SIP.1.1	The TSF shall ensure any data in the specified data resource is overwritten.

6.2 Security Assurance Requirements

The security assurance requirements for this TOE are limited to those that conform to the evaluation assurance level EAL2 specified in CC Part 3. Below specified in Table 2 are the security assurance requirements this TOE requires.

Table 2: TOE Security Assurance Requirements

Assurance classes	Assurance components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security implementation function specifications
	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	Using the CM system
	ALC_CMS.2	CM scope of a part of the TOE
	ALC_DEL.1	Delivery 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

Assurance classes	Assurance components	
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.3 Rationale for Security Requirements

This section describes the rationale behind security requirements that consist of rationale for security functional requirements, dependency verification, and rationale for security assurance requirements.

6.3.1 Rationale for Security Functional Requirements

O.OVERWRITE is the only security objective, and FDP_SIP.1 is the only security functional requirement, for this TOE. O.OVERWRITE is fulfilled by FDP_SIP.1 and corresponding relationships can be maintained between them. Therefore, all security functional requirements for this TOE are associated with at least one security objective. For this reason, security functional requirements are necessary.
Moreover, to eliminate any leakage potential of the data that is stored on the HDD area that the MFP specifies, O.OVERWRITE requires that all data in the area shall be invalid, and FDP_SIP.1 applies overwrite operation to the data in the specified area. Consequently, the requirements for O.OVERWRITE can be fully satisfied by FDP_SIP.1.

6.3.2 Dependency Verification

No dependencies are assumed for FDP_SIP.1, which represents the security functional requirements for this TOE. Accordingly, the dependency of the security requirements for this TOE is satisfied.

6.3.3 Rationale for Security Assurance Requirements

This TOE is an optional product provided with MFPs, which are commercially available. Office installation is assumed for MFPs, and malicious parties with basic attack potential are assumed. Consequently, the TOE shall ensure it can counter attacks from malicious parties with basic attack potential, which are expected to happen in general offices.

Verifications based on EAL2 certification include verification of security functions and their architecture, guidance documents that are compiled to ensure security functions are properly used, security measures that are applied to distribution routes, configuration management for configuration items, and testing based on security functions and their architecture.
These packages for verification satisfactorily ensure that the TOE can counter attacks from malicious parties with basic attack potential against general and commercially available products in offices.

Consequently, selection of EAL2 is appropriate.

7 TOE Summary Specifications

SF.OVERWRITE represents security functions that can be derived from FDP_SIP.1, security functional requirements for the TOE. Below, SF.OVERWRITE is outlined and methods specified by SF.OVERWRITE to achieve FDP_SIP.1 are defined.

SF.OVERWRITE

The TOE applies overwrite operations to the HDD area that the MFP specifies. To create the area that the MFP specifies for overwrite operations, sequential overwriting and batch overwriting are available. Details of both functions are described below:

- Sequential Overwrite Function
  When receiving overwrite instructions from the MFP, the TOE applies overwrite operations to the HDD area specified by the MFP.
- Batch Overwrite Function
  When receiving batch overwrite instructions from the MFP, the TOE applies overwrite operations to all the HDD area. The TOE also receives cancellation instructions from the MFP. Once receiving the cancellation instructions, the TOE suspends batch overwrite operations.

To overwrite data, the NSA, DoD, random number, or BSI/VSITR methods can be used. The TOE receives overwrite instructions from the MFP, which specifies which method is used for data overwriting. Brief explanations for each method are as follows (the BSI/VSITR method cannot be used for sequential overwriting):

- NSA method:
  Data overwritten twice by random numbers and once by null (0).
- DoD method:
  Data overwritten once by fixed numbers, once by their complements, once by random numbers, and the results will be verified.
- Random number method:
  Data overwritten a number of times (1 - 9 times) specified using random numbers. The MFP specifies the number of overwrite operations.
- BSI/VSITR:
  Data overwritten 7 times with 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, and 0xAA (in this order).

Achieving FDP_SIP.1

FDP_SIP.1 is the requirement to ensure that overwrite operations are applied to the data on the resource area (HDD) that the MFP, a trusted IT product, specifies.
SF.OVERWRITE achieves FDP_SIP.1 by applying overwrite operations to the HDD area that the MFP specifies for sequential or batch overwriting. For this, the method the MFP specifies can be implemented from the NSA, DoD, random number, and BSI/VSITR methods. By so doing, all data on the HDD becomes invalid. Sequential overwriting methods include NSA, DoD, and random number methods, and batch overwriting methods include NSA, DoD, random number, and BSI/VSITR methods.

8 Appendix

8.1 Glossary

Refer to Table 3 for the terms used in this ST.

Table 3: Terms Used in this ST

Terms	Definitions
MFP	A digital multi function product. A printer with multiple functions (copy, print, etc.)
SD memory card	A secure digital memory card. A highly functional memory card that is the size of a postage stamp and can be used to install the TOE and other applications on the MFP.
Document Server Function	One of the MFP functions. This function allows users to store scanned paper document data on the HDD of the MFP. In addition, by using its Copy, Print, and Document Server Functions, users can print and delete the document that is stored on the HDD of the MFP.

Annex A

Table 4 shows the name of MFPs on which this TOE is installed to use.

Table 4: MFPs used with this TOE

Product name
Ricoh MP CW2201/CW1201 series