

Secure MFP Protection Profile - Lite

Author: Yusuke OHTA, Ricoh Company, Ltd.

Date: 2004/04/13

Version: 1.0e

Revision History

Version	Date	Author	Description
1.0	2002/11/29	Yusuke OHTA	The first version in Japanese.
1.0e	2004/04/13	Yusuke OHTA	Translated into English for IEEE P2600.

Table of Contents

1	<i>PP Introduction</i>	5
1.1	PP identification	5
1.2	PP overview	5
2	<i>TOE Description</i>	6
2.1	Definition of specific terms	6
2.2	About the product	7
3	<i>TOE Security Environment</i>	9
3.1	Assets	9
3.2	Assumptions	9
3.3	Threats	10
3.4	Organisational security policies	10
4	<i>Security Objectives</i>	11
4.1	Security objectives for the TOE	11
4.2	Security objectives for the environment	12
4.2.1	Security objectives for the IT environment.....	12
4.2.2	Security objectives for the non-IT environment	12
5	<i>IT Security Requirements</i>	13
5.1	TOE security functional requirements	13
5.1.1	Security audit (FAU).....	13
5.1.2	User data protection (FDP)	14
5.1.3	Identification and authentication (FIA).....	15
5.1.4	Security management (FMT).....	16
5.1.5	Trusted path/channels (FTP).....	17
5.2	Minimum strength of function claim	17
5.3	TOE security assurance requirements	18
5.4	Security requirements for the environment	19
6	<i>Rationale</i>	20
6.1	Security objectives rationale	20
6.2	Security requirements rationale	21
6.2.1	Rationale for functional requirements.....	21
6.2.2	Rationale for minimum strength of function level.....	21
6.2.3	Rationale for assurance requirements	21
6.2.4	Mutual support of security requirements	21
7	<i>Annex</i>	22
7.1	Source	22
7.2	Abbreviation	22

List of Figures

Figure 1: Overview of the TOE, data, and users 8

List of Tables

Table 1: Specific terms in Secure MFP PP 6
Table 2: TOE security assurance requirements (EAL3)..... 18
Table 3: Correspondence between security needs and security objectives 20
Table 4: Correspondence between security objectives and functional requirements 21

1 PP Introduction

1.1 PP identification

Title:	Secure MFP Protection Profile - Lite
Version:	1.0e
Date:	2004/04/13 (The Japanese version 1.0 was written in 2002/11/29.)
Author:	Yusuke OHTA, Ricoh Company, Ltd.
CC used:	CC Ver.2.1, identical to ISO/IEC 15408:1999(E)
Keywords:	MFP, document, copier, printer, scanner, facsimile, network, office

1.2 PP overview

This Protection Profile (PP) describes an implementation-independent set of security requirements for a Multi-functional Printer (MFP), which covers assumed environment in which the MFP is operated, objectives that the MFP and its environment must achieve and IT security requirements that the MFP must meet.

The MFP is a network-connected device mainly used in office environment and provides multiple functions, e.g. copier, printer, scanner, and facsimile. As some of the objects (e.g. electronic documents, paper documents and address book) with which the MFP deals are sensitive for users, the appropriate protection for them is required. Additionally, the residual image data temporarily stored in hard-disc drives (HDD) at user operations (e.g. copy or print) should be considered as asset to be protected. Moreover, some customers worry about unauthorised intrusion via telephone line that is used for facsimile.

The Target of Evaluation (TOE) focused in this PP is a set of modules of the MFP that realise the security functions to protect the assets. When only software modules realise the security functions, the TOE consists of the software modules. When the security functions are realised by both software and hardware, the scope of the TOE also includes the hardware.

2 TOE Description

2.1 Definition of specific terms

Table 1 shows the definition of specific terms in this PP in order for readers to understand the PP easily.

Table 1: Specific terms in Secure MFP PP

Term	Meaning
<p>Assets</p> <p>Document</p> <p>User Function Data</p> <p>Management Data</p> <p>Resource</p>	<p>It includes all kind of documents with which users consciously deal, e.g. original paper to be copied, electronic files to be printed from PCs, image data sent with facsimile, stored data in the HDD of the MFP and so on.</p> <p>It indicates the user original data other than Documents that the MFP applications use, e.g. phone books for facsimile. It is distinguished from the Management Data.</p> <p>It indicates the secondary asset that is needed for the security functions of the MFP but not for users. The examples are as follows:</p> <ul style="list-style-type: none"> - user management data, e.g. password, - device management data, e.g. audit data, log data, paper configuration, - network management data, e.g. MFP IP address, server's IP address, etc. <p>From the point of view of the CC, this data is categorised as "TSF data".</p> <p>It indicates hardware modules that consist of the MFP (e.g. CPU, RAM, HDD), software modules, and the supply for the MFP (e.g. paper, toner).</p>
<p>User role</p> <p>Internal User</p> <p>Device Administrator</p> <p>Network Administrator</p> <p>Normal User</p>	<p>It indicates the entity that accesses to the MFP physically or via intranet. The Internal User includes Device Administrator, Network Administrator, Normal User, Customer Engineer and Maintenance Device. For detail of those roles, see below.</p> <p>It indicates the privileged user who performs administrative operations of the MFP other than the network configuration (e.g. management of users, resources of the MFP and audit data). The Device Administrator is one role of the Internal User.</p> <p>It indicates the privileged user who manages the network configuration of the MFP. This PP distinguishes the Network Administrator from the Device Administrator because of some users' requests. In many cases, the same person might act the two roles. The Network Administrator is one role of the Internal User.</p> <p>It indicates the user who accesses to the MFP for normal use via the Operation Panel of the MFP or via intranet (e.g. copy, print, scan). The Network Administrator is one role of the Internal User.</p>

Term	Meaning
Customer Engineer	It indicates the person who works for the vendor of the MFP and maintains it at the customer's site. The Customer Engineer is one role of the Internal User.
Maintenance Device	It indicates the dedicated device that is set in the intranet and maintains the MFP. The Maintenance Device is not a person but is considered as one role of the Internal User.
External User	It indicates the entity that accesses to the MFP from outside of the office via the Telephone Line.
Interfaces to the MFP	
Operation Panel	It indicates the panel for operations that is attached to the MFP. It typically consists of a LCD and some buttons. The Internal Users operate the MFP with the Operation Panel.
Network Interface	It indicates the interface used to connect the MFP to intranet, e.g. the ethernet interface.
Telephone Line	It indicates the interface used to connect the MFP to the public circuit for facsimile.
Miscellanea	
Temporary Data	It indicates the image data that is temporarily built on the HDD before the MFP performing operations of the Applications.
Application	It indicates the major functions that the MFP provides, e.g. copying, printing, scanning, and facsimile.

2.2 About the product

The product type of the TOE is Multi-functional Printer (MFP).

The MFP provides some Applications concerning the Documents mainly in office environment. Some kind of MFP also provides the functionality such as transferring scanned data to PCs or servers via network. And the MFP realises the advanced copying operations, e.g. integration of pages or repetition of printing, by keeping the Temporary Data in the built-in HDD.

The objects that are dealt with by the MFP and considered as assets (necessary to be protected) are primarily the Documents, the User Function Data, and the Resources (for detail, see Table 1). In addition, the Management Data needed for security functions should be considered the secondary assets and be protected appropriately.

As interfaces to the MFP, the Operation Panel for direct access, the Network Interface for remote access, and the Telephone Line for facsimile should be considered. The Internal User uses the Operation Panel and the Network Interface to access the MFP, and the External User uses the Telephone Line.

Figure 1 shows the abstract diagram concerning the TOE, data, users, and interfaces.

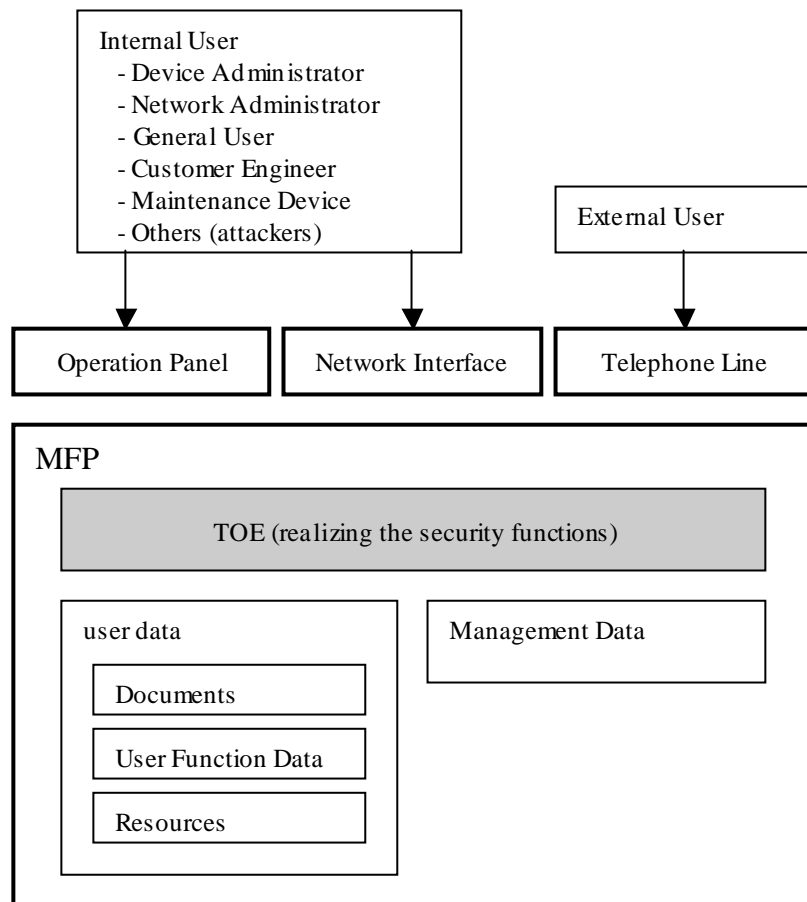


Figure 1: Overview of the TOE, data, and users

3 TOE Security Environment

3.1 Assets

The primary assets that the TOE shall protect are the Documents, the User Function Data and the Resources of the MFP. In addition, the Management Data is considered as secondary assets because it is necessary to protect it in order for the MFP to protect primary assets appropriately.

3.2 Assumptions

In this section, the assumptions that are postulated in the environment of use of the MFP are defined with identifiers (e.g. A.ADMIN). The security functions of the MFP will be designed on condition that all the assumptions are satisfied. In other words, if one or more assumptions are not fulfilled, it means there is the possibility that the assets might not be protected with the security functions of the MFP.

A.ADMIN **It is assumed that the Device Administrator and the Network Administrator of the MFP can be trusted, do not abuse their authority, and follow the instructions in the guidance documentation of the MFP.**

For example, the Device Administrator and the Network Administrator do not peep nor modify the Documents and authentication data (e.g. password) of the Normal Users maliciously. One more example, in case that there is password mechanism in the MFP, they do not use the weak passwords for themselves, e.g. all characters are same, the numbers are consecutive or words in dictionary.

A.USER **It is assumed the Normal User of the MFP follows the instructions in the guidance documentation in order to protect his/her own Documents.**

For example, the Normal User does not use the weak password, e.g. all characters are same, the numbers are consecutive or words in dictionary.

A.ACCESS **It is assumed that the MFP is not installed in general public place and that the MFP is not connected directly to the Internet.**

Only specific persons can physically access to the MFP. And the MFP is connected to the network protected by a firewall from the Internet, i.e. the network access to the MFP comes only from the intranet.

3.3 Threats

In this section, the threats to which the MFP faces in the environment assumed in this PP are defined with identifiers (e.g. T.DOC).

T.DOC **An unauthorised Internal User might access to the Documents of the other Internal Users.**

The unauthorised Internal User uses the normal interfaces (e.g. Operation Panel or Network Interface) to read, modify, delete, or carry away the Documents. Not only Normal Users but also Customer Engineers can be the attacker.

T.SALVAGE **An Internal User might read the contents of the Documents by carrying away the HDD from the MFP and analysing it.**

For example, the Internal User might salvage the residual data of the Temporary Data used for the last copy operation or access to the stored Documents by connecting the HDD to a PC.

T.NETWORK **An Internal User might read or modify the contents of the Documents by capturing the packets on the intranet.**

The Internal User might capture packets on the intranet and sniff the Documents which the other Internal Users access via the network.

T.TEL **An External User might access to the Resource of the MFP via the Telephone Line and perform the unauthorised operation.**

The External User might intrude into the MFP and might access the Documents or intrude into the other systems in the intranet by using the MFP as a springboard.

T.RESOURCE **An Internal User might use the Resource of the MFP without authorisation.**

The unauthorised Internal User might open the body of the MFP and carry away paper or toner for other use. In case that the permissions of operating the Applications for each Internal User are different (e.g. Mr. A is permitted operating copy Application but Mr. B is not, or Mr. A is permitted operating copy Application but not print Application.), the unauthorised Internal User might operate the Applications without permission, i.e. use the Resource.

3.4 Organisational security policies

There are no organisational security policies with which the MFP must comply.

4 Security Objectives

4.1 Security objectives for the TOE

In this section, the TOE security objectives which are needed to counter the threats in section 3.3 are defined.

- O.I&A** **The TOE must identify and authenticate each Internal User and External User who try to access the objects in the MFP.**
- The “object” means Document, User Function Data, Management Data, and Resource. Access to the Resource includes operating the Application of the MFP, copy or print operation.
- O.ACCESS** **The TOE must ensure that only authorised users can access the objects.**
- The TOE forces the access control policies based on the user identifier given by O.I&A. The TOE also ensures that only authorised users can modify the access control policy against each object, i.e. modification of the Management Data (e.g. ACL).
- O.DELETE** **The TOE must dispose the Temporary Data used for the Applications in order to prevent carrying away the data from the HDD just after those operations finish.**
- This “carrying away” includes salvaging the Temporary Data from the residual data on the HDD.
- O.NETWORK** **The TOE must protect the information from/to the MFP through the intranet from unauthorised disclosure.**
- The TOE must counter such attacks as peeping the packets on the network.
- O.MONITOR** **The TOE must audit the events of security-related actions by the Internal Users and the External Users, and show the audit data to the authorised users.**
- Auditing is useful for both immediate detection of the security problems and prevention of casual attacks by psychological depression effect.

4.2 Security objectives for the environment

4.2.1 Security objectives for the IT environment

There are no security objectives that the IT environment of the TOE shall achieve.

4.2.2 Security objectives for the non-IT environment

In this section, the security objectives that the non-IT environment of the TOE shall achieve to satisfy the assumptions in section 3.2 and to counter the threats in section 3.3.

OE.TRAIN Device Administrators, Network Administrators, and Normal Users must be trained to operate the MFP correctly following the guidance documentation.

They must be trained to read guidance documentation and to operate the MFP correctly, in order to protect the MFP that they administer or to protect their own Documents. Especially, in case that the password mechanism is used for the authentication, they must be trained not to use the weak passwords.

In addition, the trusted persons should be assigned as the Device Administrator and the Network Administrator, who do not peep nor modify the Documents and authentication data (e.g. password) of the Normal Users maliciously by abusing their authority.

OE.LOCATION The Device Administrator must install the MFP in physically secure place.

The MFP should be placed where only specific persons can access to the MFP physically, e.g. in office with entrance management system.

OE.NETWORK The Network Administrator must keep the intranet such secure that no external attacks exist.

The MFP should be connected to the internal network protected from the unspecified attacks from the Internet, e.g. by installing a firewall.

5 IT Security Requirements

5.1 TOE security functional requirements

In this section, the security functional requirements that the TOE must satisfy in order to achieve the security objectives defined in section 4.1. In description of the requirements, the words against which the assignment or selection operation are performed are identified with **[bold letters and brackets]**, the refinement operations are identified with **bold letters and underline**, and the iteration operations are identified with lower-case alphabetical suffix, e.g. “-a”.

The unfinished operations identified as [operation: *italic letters*] shall be completed in the Security Target (ST).

5.1.1 Security audit (FAU)

FAU_GEN.1 **Audit data generation**

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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and
- c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, 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*]

Dependencies: FPT_STM.1

FAU_SAR.1 **Audit review**

FAU_SAR.1.1 The TSF shall provide **[Device Administrators]** 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.

Dependencies: FAU_GEN.1

FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to **[prevent]** modifications to the audit records.

Dependencies: FAU_GEN.1

FAU_STG.3 Action in case of possible audit loss

FAU_STG.3.1 The TSF shall take [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

Dependencies: FAU_STG.1

FAU_STG.4 Prevention of audit loss

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

Dependencies: FAU_STG.1

5.1.2 User data protection (FDP)**FDP_ACC.2 Complete access control**

FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on **[the following subject and objects]:**

- **Subject: Internal User and External User; and**
- **Object: Document, User Function Data and Resource,]**

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on **[identity of the Internal User and External User]**.

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*].

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

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

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[deallocation of the resource from]** the following objects: **[Documents]**.

Dependencies: No dependencies

5.1.3 Identification and authentication (FIA)**FIA_AFL.1 Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] **consecutive** unsuccessful authentication attempts occur related to **[authentication for a Normal User]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[deny any authentication attempts for the Normal User]**.

Dependencies: FIA_UAU.1

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1

FIA_UAU.7 Protected authentication feedback

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

Dependencies: FIA_UAU.1

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.4 Security management (FMT)**FMT_MTD.1-a Management of TSF data**

FMT_MTD.1.1-a The TSF shall restrict the ability to [selection: *modify or clear*] the [secret for authentication] to [its owner].

Dependencies: FMT_SMR.1

FMT_MTD.1-b Management of TSF data

FMT_MTD.1.1-b The TSF shall restrict the ability to [selection: *change_default and modify*] the [permission attribute of a Document] to [its owner (Normal User)].

Dependencies: FMT_SMR.1

FMT_MTD.1-c Management of TSF data

FMT_MTD.1.1-c The TSF shall restrict the ability to [delete and [create]] the [identity of a Normal User] to [the Device Administrator].

Dependencies: FMT_SMR.1

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [Device Administrator, Network Administrator, Normal User, Customer Engineer, Maintenance Device and External User].

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

Dependencies: FIA_UID.1

5.1.5 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote 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 [**the TSF and the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transfer of the Documents and secrets for the authentication**].

Dependencies: No dependencies

5.2 Minimum strength of function claim

The minimum strength of function required in this PP is “SOF-Basic”.

5.3 TOE security assurance requirements

The assurance components for the TOE are shown in Table 2. It is the set of components defined by the evaluation assurance level **EAL3** and no other requirements have been augmented.

Table 2: TOE security assurance requirements (EAL3)

Assurance Class	Assurance Component
Security Target	ASE_DES.1 TOE description
	ASE_ENV.1 Security environment
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives
	ASE_PPC.1 PP claims
	ASE_REQ.1 IT security requirements
	ASE_SRE.1 Explicitly stated IT security requirements
	ASE_TSS.1 TOE summary specification
Configuration Management	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support	ALC_DVS.1 Identification of security measures
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.4 Security requirements for the environment

There are no security requirements for the environment in which the TOE is operated.

6 Rationale

6.1 Security objectives rationale

Table 3: Correspondence between security needs and security objectives

	O.I&A	O.ACCESS	O.DELETE	O.NETWORK	O.MONITOR	OE.TRAIN	OE.LOCATION	OE.NETWORK
T.DOC	X	X			X		X	X
T.SALVAGE			X					
T.NETWORK				X				
T.TEL					X			
T.RESOURCE	X	X			X		X	X
A.ADMIN						X		
A.USER						X		
A.ACCESS							X	X

Note: Justification for each threat and assumption why the related security objectives cover it shall be described here in the certified PP.

6.2 Security requirements rationale

6.2.1 Rationale for functional requirements

Table 4: Correspondence between security objectives and functional requirements

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FAU_STG.3	FAU_STG.4	FDP_ACC.2	FDP_ACF.1	FDP_RIP.1	FIA_AFL.1	FIA_SOS.1	FIA_UAU.2	FIA_UAU.7	FIA_UID.2	FMT_MTD.1-a	FMT_MTD.1-b	FMT_MTD.1-c	FMT_SMR.1	FTP_ITC.1
O.I&A									X	X	X	X	X				X	
O.ACCESS						X	X							X	X	X	X	
O.DELETE								X										
O.NETWORK																		X
O.MONITOR	X	X	X	X	X													

Note: Justification for each objective why related security functional requirements meet the objective shall be described here in the certified PP.

6.2.2 Rationale for minimum strength of function level

Note: This part is omitted in this PP-Lite. The reason why the minimum strength of function in section 5.2 is claimed shall be described here in the certified PP.

6.2.3 Rationale for assurance requirements

Note: This part is omitted in this PP-Lite. The reason why the EAL in section 5.3 is claimed shall be described here in the certified PP.

6.2.4 Mutual support of security requirements

Note: This part is omitted in this PP-Lite. The justification to demonstrate that the security requirements are mutually supportive and internally consistent with each other shall be described here in the certified PP.

7 Annex

7.1 Source

CC	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements
----	---

7.2 Abbreviation

CC	Common Criteria
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
MFP	Multi-functional printer
HDD	Hard-disc drive
CPU	Central processing unit
RAM	Random access memory
PC	Personal computer
LCD	Liquid crystal display
ACL	Access control list