KECS-CR-10-16

Samsung MFP Security Kit Type_B V1.0 Certification Report

Certification No.: KECS-CISS-0229-2010

April 2010

IT Security Certification Center

Revision history

No.	Date	Page	Revision
00	22 Apr. 2010	-	First draft

This document is the certification report on Samsung MFP Security Kit Type_B V1.0 of Samsung Electronics Co., Ltd.

Certification Body

IT Security Certification Center

Evaluation Facility

Korea System Assurance, Inc.

Table of Contents

1. Overview

This report describes the certification result drawn by the certification body on the results of the EAL3 evaluation of Samsung MFP Security Kit Type_B V1.0 ("TOE" hereinafter) with reference to the Common Criteria for Information Technology Security Evaluation (notified on 1 Sep. 2009, "CC" hereinafter). It describes the evaluation result and its soundness and conformity.

The evaluation of the TOE has been carried out by Korea System Assurance, Inc.(KOSYAS) and completed on 31 March 2010. This report grounds on the evaluation technical report(ETR) KOSYAS had submitted, in which the evaluation has confirmed that the product had satisfied the requirements of CC Part 2 and CC Part 3 and had been "suitable" according to the CC Part 1, paragraph 245.

The TOE is software embedded on SAMSUNG multi-function printers(MFPs). These MFPs include copy, print, scan, netscan, scan-to-email, scan-to-server, and fax features. The TOE allows the MFPs to perform image overwrite, fax/network separation, identification, authentication, and network access control tasks.

The CB has examined the evaluation activities and test procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each evaluation work package report and evaluation technical report.

Consequently, the CB has confirmed that the evaluation results had ensured that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST.

Thus the CB has certified that observations and evaluation results made by the evaluator had been correct and reasonable, and the verdicts assigned by the evaluator on the product had been correct.

Certification validity: Information in this certification report does not guarantee that Samsung MFP Security Kit Type_B V1.0 is permitted use or that its quality is assured by the government of Republic of Korea.

2. TOE Identification

[Table 1] identifies the TOE.

[Table 1] TOE identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (1 Sep. 2009) Korea IT Security Evaluation and Certification Scheme (1 Jan. 2010)
TOE	Samsung MFP Security Kit Type_B V1.0
Protection Profile	N/A
Security Target	Samsung MFP Security Kit Type_B V1.0 Security Target V1.1
ETR	Samsung MFP Security Kit Type_B V1.0 Evaluation Technical Report V1.0
Evaluation result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation criteria	Common Criteria for Information Technology Security Evaluation V3.1
Evaluation methodology	Common Methodology for Information Technology Security Evaluation V3.1
Sponsor	Yoonwoo Lee, the CEO of Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Evaluator	Jungdae Kim, Jiyeon Lee Korea System Assurance, Inc.
Certification body	IT Security Certification Center

3. Security Policy

The TOE operates in conformance with the following security policies:

P.HIPAA_OPT

In order to keep track of security-relevant actions according to HIPAA policy, the TOE should precisely leave the job history on record and safely maintain their security-relevant events, and properly go over the recorded data.

P.SAFE_MANAGEMENT

The TOE should provide a safe management tool on the Web or local user interface so that only an authorized administrator can manage the TOE in a secure manner.

4. Assumptions and Scope

4.1 Assumptions

The TOE shall be installed and operated with the following assumptions in consideration:

A.PHYSICAL_SECURITY

The TOE is protected from unauthorized physical counterfeit/camouflage in the office environment.

A.TRUSTED_ADMINISTRATOR

The authorized system administrator of the TOE has no malice, has received education about the TOE administrative functions, and should perform proper actions according to the proposed manual provided with the TOE. The local administrator should maintain the PIN and change it at least once every 40 days.

A.TRUSTED_NETWORK

The network connected to the TOE should install a firewall system between the internal and external network to block attacks from outside.

A.TRUSTED_AUTHENTICATION_SERVER

When the TOE performs client authentication for network scan services via authentication server, the authenticated server should be safely managed and provide safe remote authentication through certificated protocol.

A.TIME_STAMP

The environment of the TOE provides reliable time-stamps for accurate audit logs about the TOE.

A.SSL

SSL protocol is used to serve safe communication between the user's client PC or web system administrator's PC and TOE through a web interface. Therefore, it provides confidentiality and integrity of data transferred between TOE and the web system administrator.

4.2 Scope to Counter a Threat

The TOE provides a means appropriate for the IT environment of the TOE to counter a security threat and a means to take actions on any logical/physical attacks launched by a threat agent possessing basic expertise, resources, and motivation.

All security objectives and security policies are described such that a means to counter identified security threats can be provided.

5. TOE Information

[Table 2] and [Table 3] shows the options provided by SAMSUNG MFPs with the TOE embedded and its hardware specifications respectively.

(X means standard options; O means customized options)

Option / MFP model	Print	Copy	NetScan	Fax	Scan-to-email	Scan-to-server
SCX-5835FN SCX-5935FN	X	X	X	O	X	X

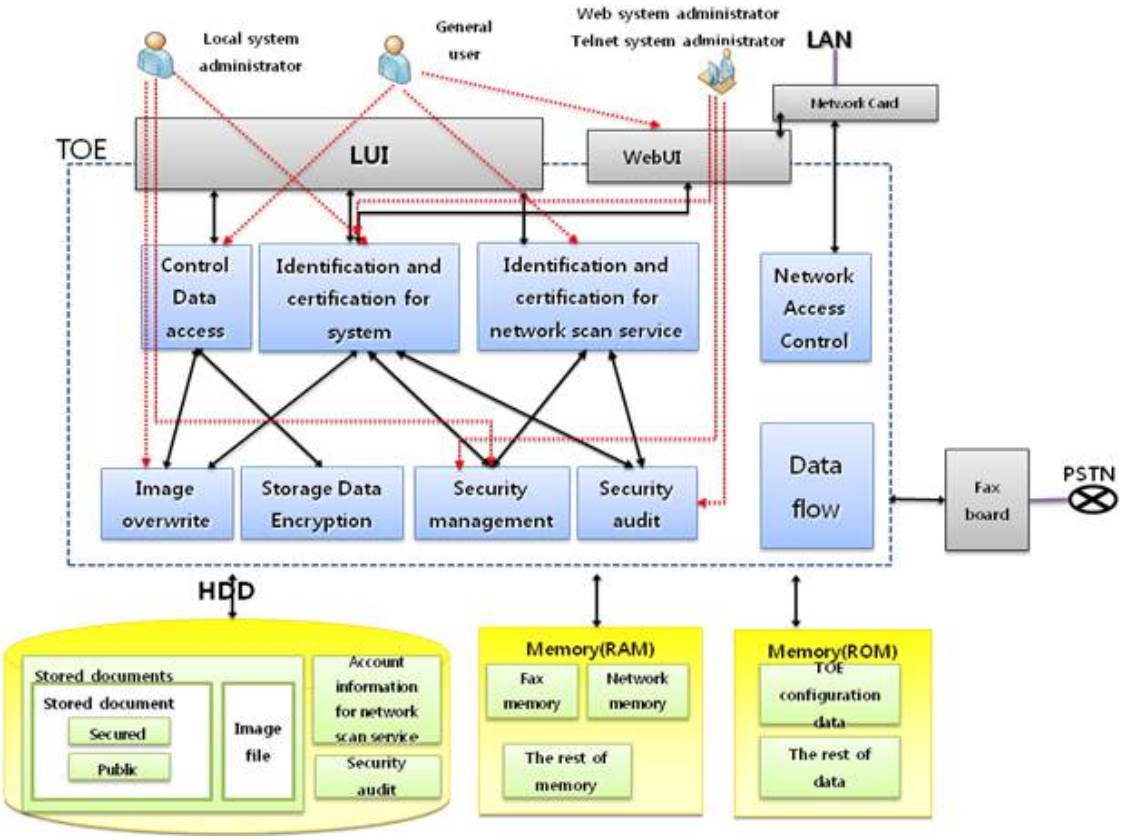
[Table 2] MFP Models and Capabilities

Specifications		SCX-5835FN/SCX-5935FN
LCD		800 x 480 7" WVGA Color Touch-Screen LCD
System Memory		256 MB & optional 256 MB
HDD		HDD (80 GB SATA)
FAX	Compatibility	ITU-T G3
	Comm. System	PSTN / PABX
	Modem Speed	33.6 Kbps
Interface		Hi-Speed USB 2.0, Ethernet 10 M / 100 M base TX
Etc.		Up to 33 ppm in A4 (35 ppm in Letter)

[Table 3] Specifications of the MFPs

The TOE operates in an internal network that is protected by a firewall system from external attacks. Users can access the TOE by using a local user interface(LUI) on an LCD of the MFP, Web user interface(WebUI) via a Web browser, Telnet interface(TelnetUI) through Telnet protocols, or a user client PC.

[Figure 1] shows the logical scope and boundary of the TOE.



[Figure 1] Logical scope of the TOE

▣ Security audit

Only authorized web administrators can download, analyze, and track the security audit log through the WebUI. The audit log provides a job owner's identification, event number, date, time, ID, description, and data to ensure credibility of the audit log. The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users (based on network login). The audit logs are available to the TOE system administrators and can be exported for review and analysis. SSL must be configured in order for the system administrator to download the audit logs; the downloaded audit logs are in a comma-separated format so that they can be imported into an application such as Microsoft Excel™.

▣ Security management

The TOE allows authorized system administrators only to use security functionality. System administrators can perform operations described below:

[Local system administrator]

- Enable or disable Automatic Image Overwrite and Manual Image Overwrite
- Start or stop Manual Image Overwrite
- Change the local administrator PIN
- Change or inquire the protocol and port

[Web system administrator]

- Configure authentication option for network scan service
- Create/Change/Delete user account for network scan service
- Change ID or password of Web system administrator and Telnet system administrator
- Enable or disable system audit log
- Download system audit log
- Change or inquire the protocol and port

[Telnet system administrator]

- Change or inquire the protocol and port

▣ System authentication

A local system administrator must be authenticated by entering a PIN prior to being granted access to the security management functions through the LUI. A security print user must be authenticated to access stored files on the TOE. A Web administrator must also be authenticated to change security management functions. The TOE displays an asterisk for each digit entered by an administrator or user to hide the value entered. Password combination rules and authentication failure handling are as follows:

[Local system administrator]

- 4 ~ 8 numerals
- In case of 3 consecutive failed authentication, a beep occurs and authentication process is delayed for 3 minutes

[Web system administrator]

- At least 1 alphabet and numeral
- 8 ~ 20 characters

- In case of 3 consecutive failed authentication, an error message is sent to the Web browser session

[Telnet system administrator]

- At least 1 upper case, lower case, and numeral
- 7 ~ 12 characters
- In case of 3 consecutive failed authentication, authentication process is delayed for 1 minute

[Security print user]

- 4 numerals
- A beep occurs every time authentication fails

▣ Network authentication

To prevent unauthorized use of the network options (netscan, scan-to-email, and scan-to-server), the TOE requires a user trying to access its network service to provide an ID and password, which are then validated by the designated authentication server. Thus, an unauthorized user cannot export stored files to the outside through network. When wrong PINs are entered 3 times in succession, the authentication process will be delayed for 3 minutes.

▣ Image overwrite

The TOE provides 2 types of image overwrite function: automatic image overwrite, which automatically overwrites temporary image files created as a result of the processing of copy/print/scan/PC-fax right after each job has been completed, and manual image overwrite, which overwrites the HDD partition where user data is stored. It performs image overwrite function as described in DoD 5200.28-M.

▣ Information flow

The TOE separates its memory into a fax memory that only the fax board can access and a network memory that only the network port in a main controller can access. Separation between the PSTN port on the FAX board and the network port on the main controller board is established through the architectural design of the main controller software. When using the fax-to-email function, the fax image received via PSTN line will be transmitted to internal network. When the fax image is proper data standardized with MMR, MR, or MH of T.4 specification, the TOE

copies the data to the network memory. (If it is not standardized, the TOE deletes it.) Then the copied fax image is transmitted to the SMTP server through a network card.

▣ Data access control

The TOE controls access to preserved files in the HDD of the MFP according to the print options set by a user. Preserved file is divided into two categories, Public and Secured. When a user stores a document as Public, all users can access and use the file. A file stored as Secured can only be accessed by the user who stored the file. When storing a file as Secured, a user must set a PIN required to access the file. Then the file can only be accessed by entering the PIN on the LUI.

▣ Storage data encryption

The TOE encrypts image data and configuration data on the HDD. After that, the TOE stores the data on the HDD and it decrypts the stored data to use it. The cryptographic algorithm used by the TOE is AES algorithm with 256-bit key size. Each product has its unique key value and stored on the MFP safely so that no one, not even the administrator, can access and leak the key value to the outside.

▣ Network access control

The TOE can control access to the TOE resources through the network from outside the TOE by changing the port number and enabling/disabling protocol. An authorized system administrator configures the protocol and changes the port number on the LUI, WebUI, or TelnetUI such that only accesses from the specified port are allowed. The administrator also controls service accesses from outside the TOE by enabling/disabling protocol.

6. Guidance

The TOE provides the following guidance documents:

- Samsung MFP Security Administrator's Guide Version 2.00 (15 Feb. 2010)
- Network Printer Administrator's Guide Version 2.00 (15 Feb. 2010)
- SCX-5835_5935 Series Multi Function Printer User's Guide Ver. 1.00 (2009. 10. 27)

7. TOE Test

7.1 Developer's Test

- **Test method**

The developer has configured the operational environment as described in the ST, where an MFP with Samsung MFP Security Kit Type_B V1.0 embedded was installed. Testing security functions was done through the TSFIs and internal interfaces of subsystems.

- **Test coverage**

All of the test cases for both functions and subsystems (56 functional tests and 18 subsystem tests) are performed to prove that the developer's test was correct.

- **Test results**

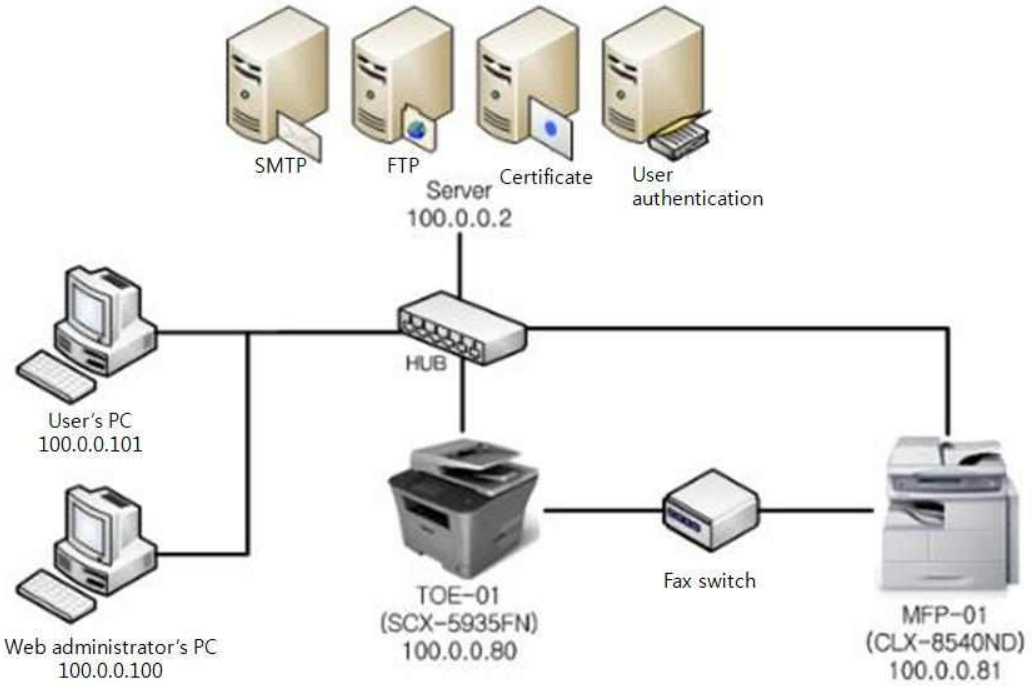
It is confirmed that the developer's test of all security functions was correct.

7.2 Evaluator's Test

The evaluator has derived test items adding to the developer's to check that the TOE operates as specified. They are described in the independent testing document in detail. The evaluator's test has proven that the TOE operates as expected.

8. Evaluation Configuration

The evaluator configured the test environment to be consistent with the developer's as shown in [Figure 2].



[Figure 2] Developer/evaluator test configuration

9. Evaluation Results

The evaluation is performed with reference to the CC V3.1 and CEM V3.1. The result claims that the evaluated product satisfies the requirements from the CC Part 2 and EAL3 in the CC Part 3. Refer to the evaluation technical report for more details.

- **Security Target evaluation (ASE)**

The ST introduction uniquely and correctly identifies the ST and TOE reference and describes the type, usage, major security features, physical and logical scope of the TOE to the extent of providing a reader general understanding.

Conformance claim includes the version of CC to which the TOE conforms, PP claim, and package claim and is described in consistent with the TOE type, security problem definition, and security objectives.

Security problem definition clearly describes the security problems that should be addressed by the TOE and its operational environment, that is, threats, organizational security policies(OSPs), and assumptions.

Security objectives counter the identified threats, achieve the OSPs, and address the assumptions properly and completely. The security problems are defined and categorized obviously into those for the TOE and for the operational environment.

The security requirements are described completely and consistently, and provides an appropriate basis for the development of the TOE to achieve the security objectives.

The TOE summary specification addresses all security functional requirements and defines them consistently with other parts of the ST.

Therefore, the ST is complete, consistent, and technically sound, and hence suitable for use as the basis for the TOE evaluation.

- **Life cycle support evaluation (ALC)**

The configuration management documentation describes that the changes to the implementation representation are controlled with the support of automated tools.

It also clearly identifies the TOE and its associated configuration items and describes that the ability to modify these items is properly controlled.

The evaluator has confirmed by examining the CM documentation that the developer had performed configuration management at least on the TOE implementation representation and evaluation evidence required by the assurance components in the ST.

Therefore, the evaluation of configuration management assists a consumer in identifying the evaluated TOE, ensures that the configuration items are uniquely identified, and guarantees the adequacy of the procedures used by the developer to control and track changes that are made to the TOE.

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing it to the user's site.

Therefore, the delivery documentation is adequate to ensure that the TOE is delivered in the same way the developer intended without modification.

The evaluator has confirmed that the developer's security controls on the development environment had been adequate to provide the confidentiality and integrity of the TOE design and implementation that are necessary to ensure secure operation of the TOE; and that the developer had used a documented life-cycle model for the TOE.

Therefore, the life-cycle support provides an adequate description of the security procedures used throughout the TOE development and maintenance.

- **Development evaluation (ADV)**

The security architecture description gives a sufficient description about the architectural properties of the TSF regarding how the security enforcement of the TSF cannot be compromised or bypassed and how the security domain provided by the TSF is separated from other domains.

The functional specification adequately describes all TSFs and explains that they are sufficient to satisfy the security functional requirements of the ST. It also adequately describes the TSFIs to the extent that a reader can understand how the TSF enforces the security functional requirements.

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. It also describes that the SFRs are completely and accurately implemented in terms of SFR-enforcing, SFR-supporting, and SFR-non-interfering interfaces.

Therefore, the development documentation is adequate to give understanding about how the TSFs are provided, as it consists of a functional specification (which describes the interfaces to the TSF), a TOE design (which describes the architecture of the TOE in terms of subsystems), and a security architecture description (which describes how the TSF enforcement cannot be compromised or bypassed).

- **Guidance documents evaluation (AGD)**

The TOE being embedded in the MFPs at the time of delivery does not apply acceptance procedures and thus does not have a preparative procedure document.

The operational user guidance describes how to administer the TOE in a secure manner.

Therefore, the guidance document gives a suitable description of how a personnel who installs, manages, and operates can administer the TOE in a secure way.

- **Tests evaluation (ATE)**

The tests have been sufficient to establish that the TSF had been systematically tested against the functional specification.

The evaluator has confirmed that the developer had tested the TSFs in the TOE design.

The developer's test documents had been sufficient to show the security functions had behaved as specified.

The evaluator has determined, after independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the developer's test results by performing all of the developer's tests.

Therefore, the tests have proved that the TSFs had satisfied the TOE security functional requirements specified in the ST and behaved as specified in the design documentation.

- **Vulnerability assessment evaluation (AVA)**

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by performing independent vulnerability analysis that the developer's analysis had been correct.

The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing an basic attack potential in the intended TOE environment.

Therefore, based on the evaluator's vulnerability analysis and penetration testing, the evaluator has confirmed that there had been no flaws or vulnerabilities exploitable in the intended environment of the TOE.

10. Recommendations

The TOE is guaranteed security only in the evaluated configuration. Therefore, one should take the following in consideration while operating the TOE.

① SSL protocol, which is provided by the operational environment for safe communication between the Web system administrator and the TOE, is disabled at the initial distribution of the TOE. So a Web system administrator should register a certificate and enable it before operating the TOE.

② The TOE is delivered with the default password of the Web system administrator and local system administrator. A system administrator who will operate the TOE should first change the password. It is recommended that Web and local system administrators change the password periodically for the sake of security.

③ Since the TOE overwrites audit data starting from the oldest one in case of exhausted audit storage, a security administrator should always check the storage status and back up the data timely to ensure traceability of security-relevant events.

11. Acronyms and Glossary

The following are the acronyms used in this report.

CC	Common Criteria
CR	Certification Report
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

The following are the terms used in this report.

Multi-Function Printer (MFP)

MFP is a machine that incorporates the functionality of multiple devices (copy, print, scan, or fax) in one.

System administrator

An authorized user who manages TOE-embedded MFP. It includes local administrator, web administrator, and Telnet administrator.

Local User Interface (LUI)

An interface for a general user or local system administrator to access, use, or manage the MFP directly.

Local System administrator

A system administrator to manage Samsung MFP Security Kit Type_B V1.0 through LUI. The main roles are to configure system information and to check the MFP status for general use. The other roles for security services

are to enable/disable Automatic Image Overwrite/Manual Image Overwrite for security, start/stop Manual Image Overwrite, and change PINs.

Web User Interface (WebUI)

An interface for a general user or Web system administrator to access, use, or manage the MFP through a web service.

Web system administrator

A system administrator to manage Samsung MFP Security Kit Type_B V1.0 through WebUI. The main roles are to create/change/delete the information of network scan service users, manage/change web administrator's ID and password, enable/disable security audit function, download security audit logs.

Telnet User Interface (TelnetUI)

An interface for a Telnet system administrator to access, use, or manage the MFP through Telnet protocols.

Telnet system administrator

A system administrator to manage Samsung MFP Security Kit Type_B V1.0 through TelnetUI. The main roles are to inquire/change the protocol and port number.

HIPAA(Health Insurance Portability and Accountability Act)

Policy that creates and reviews the records about performed job in system using hardware, software, and procedural mechanism to monitor potential violation of security rules.

12. Reference

The certification body has used the following documents to produce this certification report:

[1] Common Criteria for Information Technology Security Evaluation V3.1

[2] Common Methodology for Information Technology Security Evaluation V3.1

[3] Korea IT Security Evaluation and Certification Guidance (1 Sep. 2009)

[4] Korea IT Security Evaluation and Certification Scheme (1 Jan. 2010)

[5] Samsung MFP Security Kit Type_B V1.0 Security Target V1.1 (25 Mar. 2010)

[6] Samsung MFP Security Kit Type_B V1.0 Evaluation Technical Report V1.0 (31 Mar. 2010)