KECS-CR-08-51

Samsung MFP Security Kit Type_A V1.0
Certification Report

Certification No.: KECS-CISS-0134-2008

December 2008

National Intelligence Service

IT Security Certification Center

Revision history

No.	Date	Page	Revision
00	22 Dec. 2008	–	First draft

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

Certification Committee Members

Y. H. Jang (MOPAS), I. J. Yoon (NSRI),

H. J. Lee (Korea university), H. B. Yoo (Kwangwoon university) ,

D. H. Won (Sungkyunkwan university), K. S. Lee (Soongsil university),

J. H. Song (Hanyang university), S. W. Son (ETRI), H. S. Lee (KIISC)

Certification Body

IT Security Certification Center, National Intelligence Service

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_A V1.0(“TOE” hereinafter) with reference to the Common Criteria for Information Technology Security Evaluation (notified on 16 July 2008, "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. and completed on 5 Dec. 2008. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted, according to which the TOE has been confirmed to satisfy the CC Part 2 and Part 3 requirements and hence to be “suitable.”

The TOE is a software module loaded onto an MFP(multi-function printer) that provides functions including copy, print, NetScan, scan-to-email, scan-to-server, and fax features. The TOE allows the MFP to perform image overwrite, fax/network separation, identification and authentication.

The Certification Body 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 Certification Body has confirmed that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST. Thus the Certification Body has certified that the evaluation, including the observations of the evaluators, had been performed correctly and appropriately.

Certification validity: Information in this certification report does not guarantee that the TOE is permitted use or that its quality is assured by the government of Republic of Korea.

2 TOE Identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (No.2008−27 notified by the MOPAS, 16 Jul. 2008) Korea IT Security Evaluation and Certification Scheme (1 Sep. 2008)
Evaluated Product	Samsung MFP Security Kit Type_A V1.0
Protection Profile	N/A
Security Target	Samsung MFP Security Kit Type_A V1.0 Security Target Version 1.7 (9 Oct. 2008)
Evaluation Technical Report	Evaluation Technical Report of Samsung MFP Security Kit Type_A V1.0 (5 Dec. 2008)
Evaluation Result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V3.1 (No.2008−26 notified by the MOPAS, 16 Jul. 2008)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 Revision 2, Sep. 2007
Sponsor	Samsung Electronics, Co., Ltd.
Developer	Samsung Electronics, Co., Ltd.
Evaluator	Yongjoon Choi, Mikyoung Kim, Jungdae Kim, and Yeowung Yun(16 Jun. 2008 ~ 7 Aug. 2008) Korea System Assurance, Inc
Certification Body	IT Security Certification Center, National Intelligence Service

3 Security Policy

The TOE operates in conformance with the following security policy:

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

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 permitted system administrator in 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 a 4-digit to 8-digit PIN for key maintenance and change the PIN at least once every 40 days.

A. TRUSTED_NETWORK
The network connected to the TOE should install a firewall system to block attacks the internal from outside the network.

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
When it comes to downloading the system audit of the TOE, in order to counterfeit/camouflage the system audit of the TOE, the device transfers audit log using safe channel SSL protocol.

4.2 Scope to Counter a Threat

Threat agents are IT entities or users that can adversely access to the internal asset or harm the internal asset in an abnormal way. The threat agents have 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 Product Information

The MFP on which the TOE is loaded can be described as:

(X – Provided by default; O – Added by an order)

Function Model	Print	Copy	NetScan	Fax	Scan-to-email	Scan-to-server
SCX-6345N SCX-6345NG	X	X	X	O	X	X
SCX-6555N SCX-6555NG	X	X	X	O	X	X
CLX-8380ND CLX-8380NDG	X	X	X	O	X	X

[Function of MFP on which the TOE is loaded]

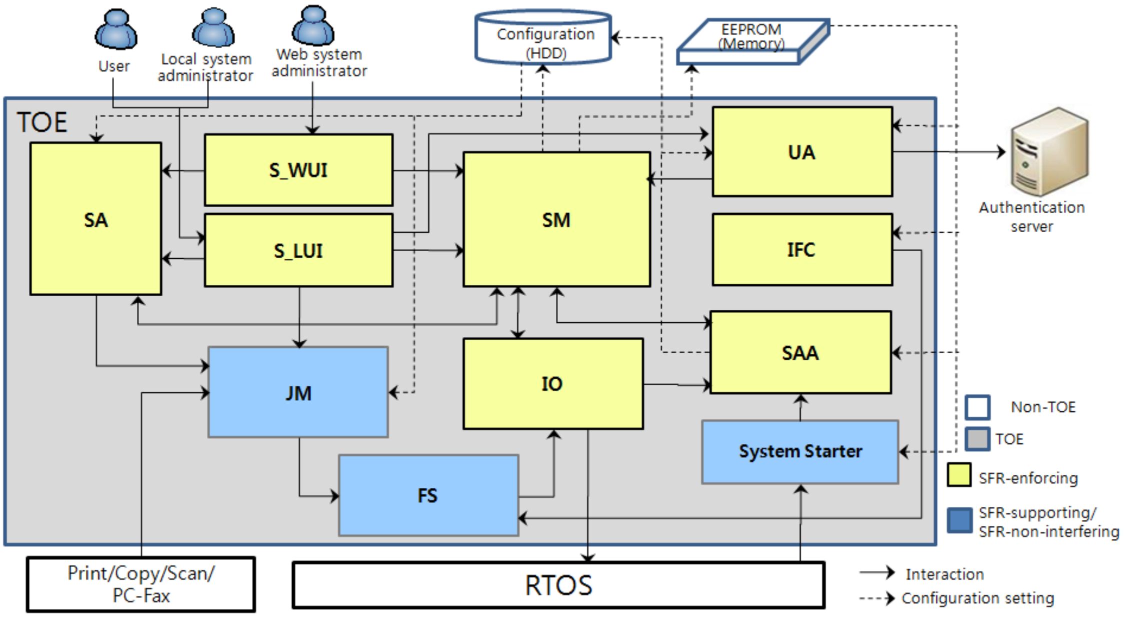
The TOE operates in an internal network that is protected from external attacks by a firewall. A user is able to access the TOE by using a local user interface(LUI) provided on the LCD of the MFP, Web user interface(WebUI) that allows remote access through the Web browser, and a user client PC.

LUI is provided to general users and local system administrator. Users can operate copy, scan, and fax through the LUI. In the case of scan, users transfer the data after the work is done to an email address, server, or user client PC through an internal communication network. A local system administrator can enable/disable IIO(Immediate image overwrite) and ODIO(On demand image overwrite), start/stop ODIO, and change administrator authentication information such as a PIN code.

WebUI is provided to a Web system administrator through the Web browser on a Web system administrator PC. An administrator can generate/modify/delete a user account, change the administrator's ID and password, enable/disable the security audit service, and download security audit files.

A general user can print out documents using a user client PC that locates in an internal network.

The follow figure shows the subsystems that comprise the TOE and their interrelationships.



[Architecture of the TOE]

The TOE comprises 11 subsystems: Security management(SM), Security Web system interface(S_WUI), Security system interface(S_LUI), System authentication(SA), Network scan service user authentication(UA), Image overwrite(IO), Information flow control(IFC), Security audit(SAA), Job management(JM), File system(FS), and System Starter subsystem. FS and JM are SFR supporting subsystems and System Starter SFR–non–interfering. The rest 8 are SFR–enforcing.

- IO subsystem

IO subsystem provides IIO, which overwrites temporary image data and stored image data used in MFP processes(copy, print, scan, or PC–fax) immediately after the work is finished; and ODIO, which overwrites all image data stored in the HDD when an authorized local system administrator demands via the LUI.

Category	Description
IIO	IO starts with receiving the file name to be overwritten from FS subsystem at the termination of an MFP task using the HDD. The following lists are the subject of IIO: - Spool data and stored image data created during print process - Stored image data created during copy process - Stored image data created during scan process - Temporary image data and stored image data created during fax transmission Print spool data and fax temporary image data are overwritten at the time of generation; other stored image data are overwritten when a user requires after performing an MFP task using the stored data through the LUI. IO function obtains cluster information of the file to be overwritten from FS subsystem and overwrites 3 times using the overwrite patterns(0x35, 0xCA, 0x97). IO subsystem sends the cluster information and overwrite patterns to the underlying OS(RTOS, Real Time Operating System) and requires overwriting. When overwriting is done, it samples 30% of the domain and checks whether it is written in the last overwrite pattern. In the case that image overwrite is failed, it displays a failure result on the LUI and Report; if it is succeeded, it displays a success result. The result of image overwrite is transmitted to SAA subsystem to generate a log.
ODIO	When the local system administrator orders ODIO through the LUI, SM subsystem stops all processes of the MFP and sends the order to IO subsystem. ODIO operates in 2 ways according to the HDD Partition: - MFP without HDD Partition(SCX6345N/SCX6345NG): Overwrite a cluster in which the data to be overwritten is stored using the location information of the cluster. - MFP with HDD Partition(SCX6555N/SCX6555NG, CLX8380N/CLX8380NDG): Overwrite all clusters of the 2 Partitions in which the data to be overwritten is stored among 3 type of Partitions. ODIO overwrites domain except the TSF data such as configuration data

	and log. It employs the same method as IIO. When the local system administrator requires IO to stop through the LUI in the middle of ODIO, IO subsystem stops its process.

- SA subsystem

SA subsystem provides a function to authenticate the local system administrator and security printing user who access the TOE through the LUI. 'Security printing user' is a general user who requires print function of the MFP via the user client PC, sets 'security printing' option, and sends a PIN Code with the printing file. When the user accesses the printing file stored in the MFP through the LUI, authentication is performed by the PIN Code. SA subsystem also provides identification and authentication of the Web system administrator who accesses the TOE through the WebUI.

Category	Description
Local system administrator authentication	When authentication of the local system administrator is required through the LUI, S_LUI subsystem requires the password from SA subsystem, which reads the password information stored in the EEPROM(Memory) and transfers it. When a security printing user requires review and printing of the stored security printing list through the LUI, S_LUI subsystem requires the list and PIN Code from SA subsystem. Then SA subsystem requires them from JM subsystem and transfers them to S_LUI subsystem.
Web system administrator authentication	When modification of configuration is required through the WebUI, identification and authentication of the Web system administrator is necessary. S_LUI subsystem sends the input ID, password, and configuration setting to SA subsystem, which will compare them with the Web system administrator ID and password stored in the EEPROM. When they match, it sends the configuration setting to SM subsystem and a login success result to S_WUI subsystem. When they do not match, it sends a login failure result to S_QUI subsystem and, if the failure exceeds 3 times, sends an error message.

- UA subsystem

When a general user requires for access to the network scan service resources, UA subsystem provides an identification and authentication function to ensure that only authorized users can use the resources. The function includes 'local user authentication' that is provided by the TOE and 'network user authentication' that uses authentication result through the external authentication servers(LDAP, SMB, and Kerberos).

Category	Description
Local user authentication	When a user requires scan process through the LUI, UA subsystem confirms the authentication data in the EEPROM and, if the setting is local user authentication, displays a local user login box. It compares the ID and password sent from S_LUI subsystem with those in the EEPROM and sends a result to S_LUI subsystem; an authentication success result if they match and an authentication failure result if they don't.
Network user authentication	When a user requires scan process through the LUI, UA subsystem confirms the authentication data in the EEPROM and, if the setting is network user authentication, displays a network user login box. Then it transfers the ID and password sent from S_LUI subsystem to the external authentication server. When it receives an authentication result from the server, it sends it to S_LUI subsystem.

- SAA subsystem

SAA subsystem provides a function to generate and store a log on security-relevant events. Format of log will be consistent with each event of MFP processes(copy, print, scan, or PC-fax), IIO, ODIO, and power on/off of the MFP. Files will be stored in the HDD, which allows 15,000 logs to be stored. If the number of logs excess the limit, the oldest log will be overwritten.

When an authorized Web system administrator requires for downloading log files through the WebUI, the request will be sent to S_WUI subsystem, SM subsystem, then SAA subsystem, which will read the required log file from the

HDD and send it. Its transmission will be through open s니, the channel provided in the IT environment.

- SM subsystem

SM subsystem provides a function to manage the TSF data that is used in IO, security audit, network scan service user authentication, and system authentication; a function to send a request for ODIO function through the LUI to IO subsystem; and a function to transfer a request for downloading logs to SAA subsystem.

Category	Description
TSF data management	When the local system administrator or Web system administrator tries to set and modify the TSF data through the LUI or WebUI, SM subsystem receives it and stores it in the HDD or EEPROM. The stored configuration data will be used by other subsystems performing the security functions.
ODIO management	When the local system administrator requires ODIO through the LUI, SM subsystem transfers the command for ODIO to IO subsystem.
Log download management	When the Web system administrator requires an order to download logs through the WebUI, SM subsystem transfers the order to SAA subusystem.

- IFC subsystem

IFC subsystem is to check whether fax data transmitted to the MFP through PSTN(Public Switched Telephone Network) follows the fax image standard (e.g. MH/MR/MMR format) prior to its transmission by fax-to-email function to the internal network where the TOE locates. If it doesn't, it simply deletes the data without storing. It transfers only standardized data. 'Fax-to-email' is a function to send fax data that the MFP received to a specified email.

- S_LUI subsystem

S_LUI subsystem provides a function to send a request for security management and authentication of a network scan service user required through the LUI to an appropriate subsystem. When authentication of the local system administrator is required through the LUI, it compares the input password with the local system administrator password received from SA subsystem. If they match, it displays security management menu; if they don't, it displays an authentication failure message and stores the number of failure in a temporary memory. In the case of more than 3 failures in the memory, it locks the authentication process for 3 minutes.

- Security Web system interface(S_WUI) subsystem

S_WUI subsystem provides a function to send a request for security management, identification and authentication of Web system administrator required through the WebUI to an appropriate subsystem. Password input through the WebUI is displayed in asterisk while authentication is in progress.

- FS subsystem

FS subsystem provides a function to manage the temporary image data created during MFP processes(copy, print, scan, or PC-fax) and the image data stored by print options. When IFC subsystem requires an email transfer after checking fax image standard, it provides a function to send required data to the network.

- Job management(JM) subsystem

JM subsystem manages the temporary files stored during MFP processes(copy, print, scan, or PC-fax). If a security printing user requires the stored security printing file list, it provides a function to transfer the file list and PIN Code to SA subsystem.

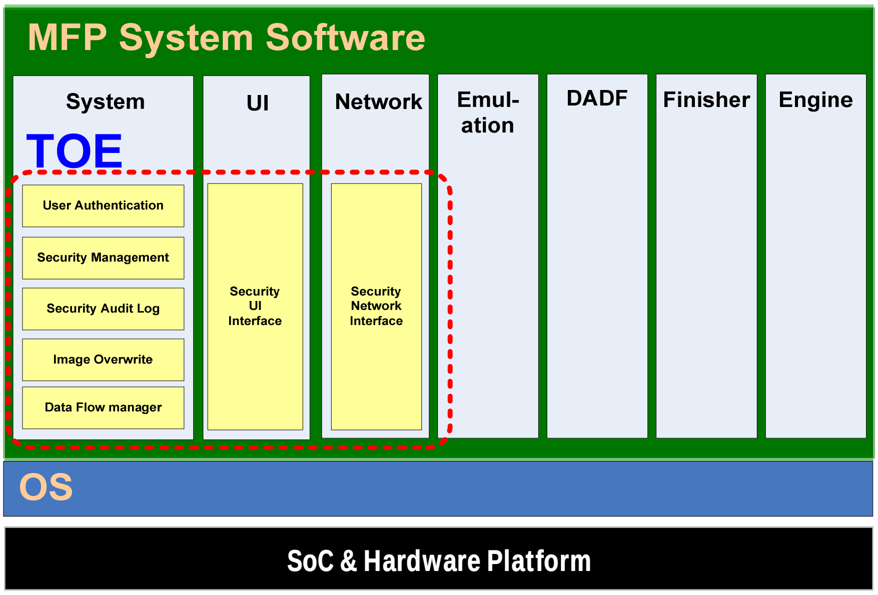
- System Starter subsystem

Once the power is on, System Starter subsystem provides functions to manage series of booting processes related to initialization of system port, timer, memory, and driver(device driver such as a scanner, HDD, or fax) and to initialization and enabling of all tasks to be performed on the firmware. If power supply is cut during IO process and the MFP is rebooted, System

Starter subsystem sends an order to IO subsystem to carry out IO function again.

[Physical scope and boundaries]

The internal structure of the MFP system software hierarchically consists of a hardware platform, an operating system (OS) that includes a device driver, and software that performs the MFP functions.



[Physical structure of MFP system software]

An underlying OS including a device driver locates on the hardware platform. The software that perform the MFP functions – System, UI, Network, Emulation, DADF, Finisher, and Engine software – operate on the OS.

The TOE is comprised of the security software module that locates in the System, UI, and Network software and the guidance documents that comes in a CD, which include the user guide, troubleshooting guide, security administrator's guide, and network printer administrator's guide.

Software comprising the TOE are listed below:

MFP Model Software	SCX-6345N SCX-6345NG	SCX-6555N SCX-6555NG	CLX-8380ND CLX-8380NDG
System Software	1.03.00.60KR_CC 12-03-2007	V2.01.00.10 05-15-2008	V2.01.00.15 05-12-20
User Authentication	TSF_SUA_V1.0	TSF_SUA_V1.0	TSF_SUA_V1.0
Security Management	TSF_SFM_V1.0	TSF_SFM_V1.0	TSF_SFM_V1.0
Security Audit Log	TSF_SAA_V1.0	TSF_SAA_V1.0	TSF_SAA_V1.0
Image Overwrite	TSF_IOW_V1.0	TSF_IOW_V1.0	TSF_IOW_V1.0
Data Flow Manager	TFS_FLW_V1.0	TFS_FLW_V1.0	TFS_FLW_V1.0
UI Software	JF_PL_V1.01.00.60 04-03-2008	V1.00.01.26 05-15-2008	V1.00.01.25 05-07-2008
Security UI Interface	TSF_LUI_V1.0	TSF_LUI_V1.0	TSF_LUI_V1.0
Network Software	V2.03.04(SCX-6345N) 04-08-2008	V4.01.04A(SCX-6x55) 05-16-08	V4.01.02A(CLX-8380) 05-16 2008
Security Network Interface	TSF_WUI_V1.0	TSF_WUI_V1.0	TSF_WUI_V1.0

[Software comprising the TOE]

- System software

It transforms the user data input by a general user into an appropriate format that can be used by the MFP. It also manages and processes the stored files. Data created during printing, scanning, or copying is completely overwritten by the IO function right after the job is finished. It performs audit function on the security-relevant events and provides the local and Web system administrators with a function to manage the security functions and TSF data.

- UI software

It provides an interface by which the local system administrator and general user can access the TOE and the TOE-embedded MFP functions through the LUI. It performs authentication function when a user tries to access the TOE through the LUI.

- Network software

It authenticates the Web system administrator and provides security functions through the WebUI. It includes a Web server, which has functions such as security management through the WebUI, log download, and Web system administrator account management. It provides network scan service to authorized users.

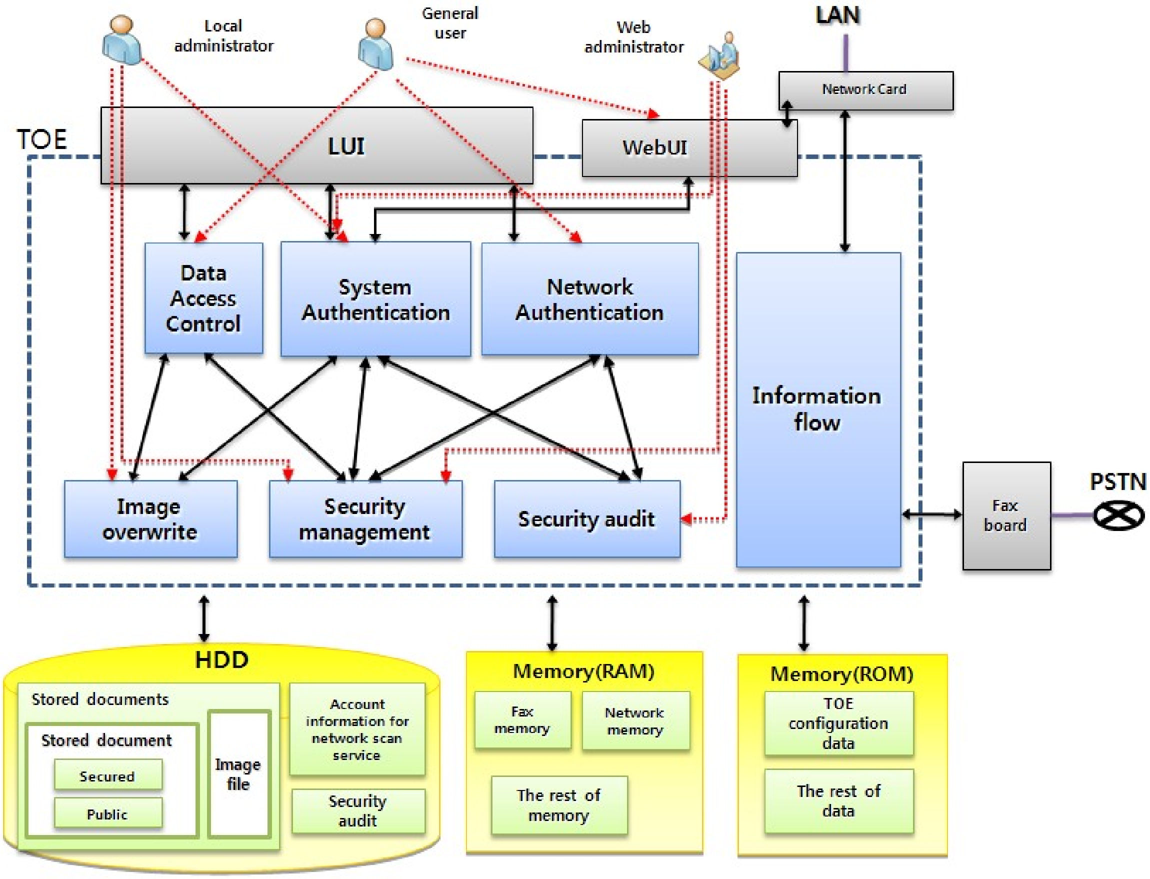
Emulation, Finisher, DADF, and Engine software are the software components used in operation of the basic MFP functions, which are categorized into H/W environment. Those are not the target of evaluation since they are not directly related to the security functions of the TOE. The MFP hardware is not in the TOE scope. The following is the hardware specification of the TOE-embedded MFP.

Specifications		SCX-6345N, SCX-6345NG	SCX-6555N, SCX-6555NG	CLX-8380ND, CLX-8380NDG
LCD		VGA (640x240) 8.4” Graphic LCD (with TSP)	WVGA (800x480) 7” TFT color LCD (with TSP)	WVGA (800x480) 7” TFT color LCD (with TSP)
System Memory		256MB Max. 384MB	Std.256MB Max. 512MB	Std.320MB (Main, 256MB + Graphic,64MB) Max. 832MB(Main, 256MB + Graphic, 64MB + Option, 512MB)
HDD		40GB IDE	80GB SATA	80GB SATA
FAX	Compatibility	ITU-T G3	ITU-T G3	ITU-T G3
	Comm. System	PSTN / PABX	PSTN / PABX	PSTN / PABX
	Modem Speed	33.6Kbps	33.6Kbps	33.6Kbps
Interface		Hi-Speed USB 2.0, Ethernet 10/100 base TX	Hi-Speed USB 2.0, USB host 1.1, Ethernet 10/100 base TX	Hi-Speed USB 2.0, USB host 1.1, Ethernet 10/100 base TX

[Hardware specification of the TOE-embedded MFP]

[Logical scope and boundaries]

The following figure shows the logical scope and boundaries of the TOE:



[Logical scope and boundaries of the TOE]

- Security audit

The TOE generates an audit log of security-relevant events, which will include a subject identity, event number, date, time, ID, description, and data to give reliability to it. An authorized Web system administrator can download the stored audit log through the WebUI for checking and analyzing. Download will only be possible by the SSL communication provided by the operational environment.

- Security management

The security functions of the TOE can only be used by an authorized local system administrator and Web system administrator. Each administrator can use the functions as below:

[Local system administrator]

- Enable/disable IIP/ODIO
- Start/stop ODIO
- Change the local system administrator password

[Web system administrator]

- Change authentication option for network scan service
- Change a local user's information for network scan service
- Change the Web system administrator ID and password
- Enable/disable security audit function
- Download security audit records

- System authentication

The TOE requires authentication of a local system administrator via the LUI prior to permitting access to the administrator security functions. It also requires authentication when a security printing service user asks for access to the stored print files and authentication of a Web system administrator when a user intends to modify the security functions through the WebUI. In all cases, the input authentication data will be displayed as asterisk('*'). Password combination rules and authentication failure handling of each administrator and user are as follows:

[Local system administrator]

- 4~8 figures
- Alarm and 3 minutes of authentication delay in case of 3 consecutive authentication failures

[Web system administrator]

- At least more than one alphabet and one figure
- 8~20 bytes
- In case of 3 consecutive authentication failures, send an error message

[Security printing user]

- 4 figures
- Alarm for each failed authentication

- Network authentication

The TOE authenticates a general user who requires a function to send scanned data to the network (e.g. NetScan, scan−to−email, scan−to−server) to prevent unauthorized users from leaking the files stored in the TOE through the network. It requires the user to enter an ID and password prior to allowing transmission of scanned data.

- Image overwrite

The TOE implements an IIO function to overwrite stored image data or temporary image data created during MFP processes(copy, print, scan, or PC−fax). It also implements an ODIO function to overwrite the HDD in which the MFP users' data is stored. Overwrite is carried out using a three pass overwrite procedure as described in the DoD 5200.28−M standard, which makes it impossible to recover.

- Information flow

The TOE divides its memory into a fax memory that the fax board of the MFP can access and a network memory that the network port of the main controller can use. Separation between the two is established through the architectural design of the main controller software. The TOE controls information flow between the two memory domains. 'Fax to email' allows the fax image received via PSTN to be transferred to the internal network. If the fax image stored in the fax memory is a standardized one such as MMR, MR, or MH image standard of T.4 specifications, the TOE copies it into the network memory, which will be transferred to the SMTP server through a network card. If it is not a standardized one, the TOE deletes it.

- Data access control

The TOE controls access to the files stored in the HDD by options during printing task. A file can be stored in the HDD either as Public or as Secured. A public file can be accessed by any user, but a secured file requires user authentication by the PIN Code set by a user who stored it.

6 Guidance

The TOE provides the following guidance documents:

1) Samsung MFP Security Administrator's Guide SCX-6345N, SCX-6345NG /SCX-6555N, SCX-6555NG /CLX-8380ND, CLX-8380NDG V 1.03
2) User Guide / Troubleshooting Guide Rev.3.00
3) Network Printer Administrator's Guide Version 1.00

7 TOE Test

7.1 Developer's Test

[Test method]

The developer derived test cases regarding the security functions of the product, which are described in the tests. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- Test purpose: Includes the security functions and modules to be tested
- Test configuration: Details about the test configuration
- Test procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator has assessed the appropriateness of the developer's test configuration, test procedures, analysis of coverage, and detail of testing and verified that the test and its results had been suitable for the evaluation configuration.

[Test configuration]

The test configuration described in the tests includes details such as network configuration, evaluated product, server, test PC, or test tools required for each test case.

[Analysis of coverage / testing: basic design]

Details are given in the ATE_COV and ATE_DPT evaluation results.

[Test result]

Tests describe expected and actual test results of each test case. The actual result can be checked on the screen of the product and also by audit log.

7.2 Evaluator’s Test

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results.

The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

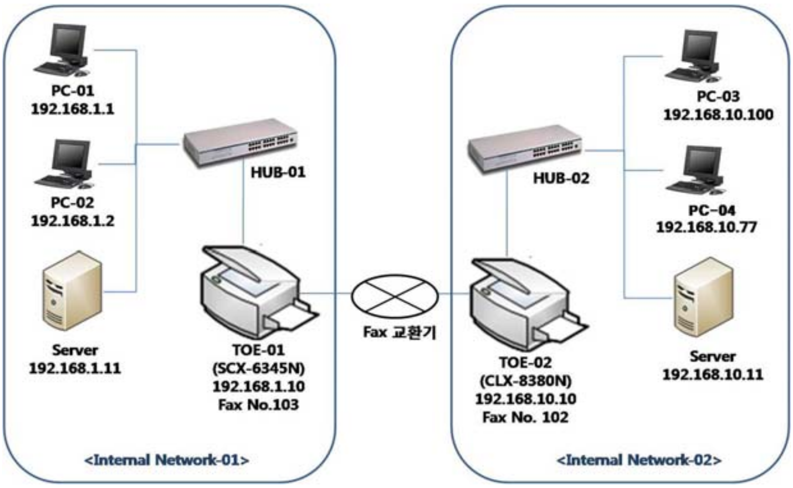
The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8 Evaluation Configuration

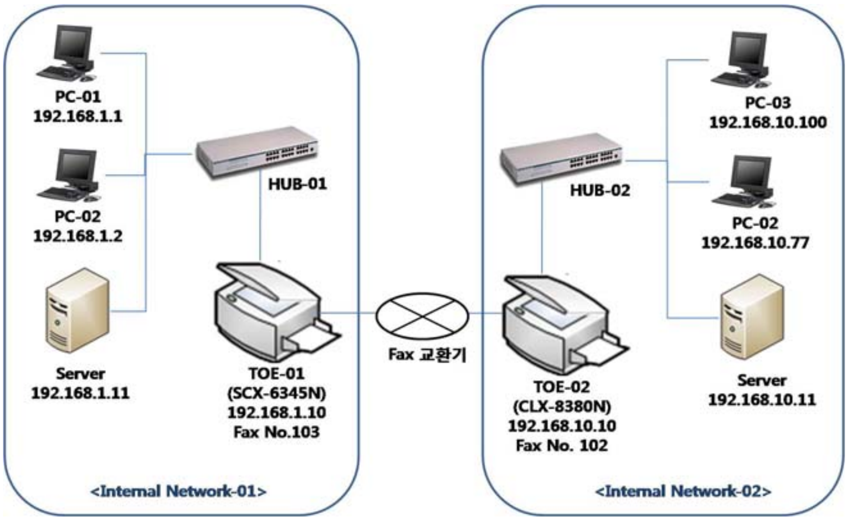
(1) Developer's test configuration

The evaluator configured the test environment as consistent with that specified in the ST as the following figure:



(2) Evaluator's test configuration

The evaluator configured the environment for the independent testing as consistent with that specified in the ST as the following figure.



9 Evaluation Result

The TOE conforms to the CC Part 2 and Part 3
And satisfies the EAL3 requirements

9.1 ST 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 assumtions.

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 provide 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.

9.2 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 security functions of the TOE and that the functions are sufficient to satisfy the security functional requirements of the ST. It also adequately describes the TSFIs(TSF interfaces) to the extent that a reader can understand how the TSF satisfies the TSP.

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 the SFR-enforcing, SFR-supporting, and SFR-non-interfering subsystems.

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 of 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).

9.3 Guidance Documents Evaluation (AGD)

The TOE does not include preparative procedures because acceptance procedures are not applicable as it is delivered securely being installed on an MFP.

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

Therefore, the guidance documents give a suitable description of how the personnel who manage and operate the TOE can administer the TOE in a secure way.

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

Therefore, the evaluation of configuration management assists the consumer in identifying the evaluated TOE, ensures that the configuration items are uniquely identified, and ensures the adequacy of the procedures that are 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 the TOE 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 confirmed that the developer's control of the development environment had been suitable to provide the confidentiality and integrity of the TOE design and implementation required for the secure operation of the TOE and that the developer had used a documented life-cycle model.

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

9.5 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 security

functions of the TOE regarding the TOE design.
The developer's test documents have been sufficient to show the security functions had behaved as specified.
The evaluator has determined, by independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the test results by performing all of the developer's tests.

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

9.6 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 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 a 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 for the TOE.

10 Recommendations

- In the case of MFP without HDD Partition(SCX6345N/SCX6345NG), the cluster information should be recorded in a table when temporary image data is generated in order to perform ODIO. Temporary image file that is created while ODIO is disabled is not the subject of image overwrite and will be deleted by the method provided by the underlying OS. Therefore, ODIO shall always be enabled to ensure that image overwrite is being applied to all temporary image data.

- If the communication channel between the Web system administrator PC and the TOE is not secure, the audit data download function is disabled. Therefore, the Web system administrator shall set the communication as 'HTTPS' to review audit data.

- The TOE overwrites the oldest audit data in case of the storage exhaustion; therefore, the security manager should check the capacity regularly and backup before the data is deleted.

11 Acronyms and Glossary

The following terms are used in this report:

(1) Acronyms

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OR	Observation Report
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

(2) Glossary

Object

A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Attack potential

A measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

Network Scan Service

This is a service that transmits scanned data to a PC on internal network, email, or FTP server through network. It includes NetScan, scan-to-email, scan-to-server.

LUI, Local User Interface

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

Local System administrator

A system administrator to manage Samsung MFP Security Kit Type_A V1.0 through LUI. The main roles are to configure system information, check MFP status for general use. The other roles for security service are enable/disable IIO/ODIO for security, start/stop ODIO, change PIN.

Security printing

When user stores a file in the HDD of the MFP from a user client PC, the user must set security printing configuration and assign PIN on the file. Then the user can access the file by entering PIN through the LUI of the MFP.

ODIO, On Demand Image Overwrite

The ODIO function overwrites all stored files including image files and preserved files on the hard disk drive, and the function should only be manually performed by a local administrator through local user interface. The image data is completely overwritten three times according to the DoD 5200.28-M standard.

Scan to server

This is a function to transmit scanned data to a remote server from the LUI. Only authorized network scan service users can use this function.

Scan to e-mail

This is a function to transmit scanned data to a remote email server from the LUI. Only authorized network scan service users can use this function.

WebUI, Web User Interface

Interface for a Web system administrator and general user to access, use, or manage the MFP through Web services.

Web System administrator

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

Image file

Files temporarily stored in the HDD of the MFP, which have user data input during scan, copy, or fax job processing transformed into a format that can be processed by the MFP.

Authorized Administrator

An authorized user with delegated authority of managing the TOE.

Authorized user

A user who may, in accordance with the SFRs, perform an operation.

Authentication Data

Information used to verify the claimed identity of a user.

Assets

Entities that the owner of the TOE presumably places value upon.

Subject

An active entity in the TOE that performs operations on objects.

IIO, Immediate Image Overwrite

IIO automatically carries out overwriting operations on temporary image files at the end of each job such as copy/print/Netscan, scan-to-email, or scan-to-server. IIO overwrites on the files in the HDD when a user initiates a delete operation on the preserved files. The image data is completely overwritten three times by using DoD 5200.28−M standard.

DoD 5200.28−M

DoD 5200.28−Mis an image overwriting standard that Department of Defense recommends. The image data in storage device is completely overwritten three times with overwriting '0x35' at first time and then '0xCA' at second time. Finally overwriting '0x97'.

MFP(Multi−Function Printer)

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

MH(Modified Huffman)

Abbreviation of Modified Huffman coding. This is encoding method to compress for storing TIFF type file. It is mainly used for fax transmission.

MR(Modified Read)

Abbreviation of Modified READ Coding; includes Modified Relative Element Address Designate MH coding.

MMR(Modified Modified Read)

Abbreviation of Modified Modified READ coding; more advanced type than MR coding.

T.4

Data compression specification for fax transmission by ITU−T(International Telecommunication Union)

12 Reference

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

1) Common Criteria for Information Technology Security Evaluation (Notification no.2008-26 of the MOPAS, 16 Jul. 2008)
2) Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2006-09-001, Version 3.1 Revision 1, Sep. 2006
3) Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2007-09-002, Version 3.1 Revision 2, Sep. 2007
4) Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2007-09-003, Version 3.1 Revision 2, Sep. 2007
5) Common Methodology for Information Technology Security Evaluation, CCMB-2007-09-004, Version 3.1 Revision 2, Sep. 2007