KECS-CR-10-65

Samsung MFP Security Kit Type_E V1.0 Certification Report

Certification No. : KECS-CISS-0278-2010

November 2010

IT Security Certification Center

Revision history

No.	Date	Page	Revision
00	9 Nov. 2010	-	First draft
01	28 Nov. 2011	3	Modify the conformance to Protection Profiles

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

Certification Committee Members

C. S. Kim (NSRI),

J. I. Lim (Korea university), D. H. Won (Sungkyunkwan university),

K. J. Chae (Ewha womans university), J. C. Ha (Hoseo university)

Certification Body

IT Security Certification Center

Evaluation Facility

Korea Security Evaluation Laboratory, Inc.

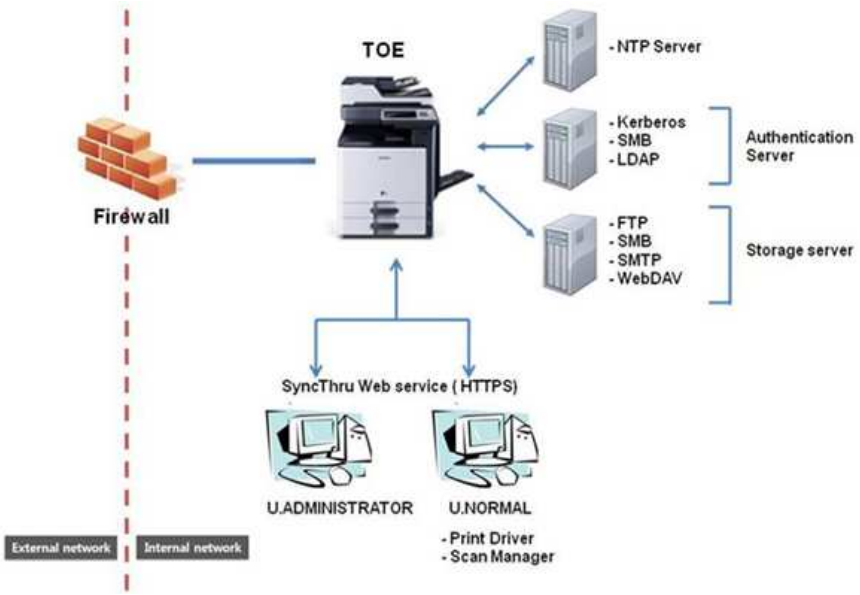
Table of Contents

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_E V1.0("TOE" hereinafter) with reference to the Common Criteria for Information Technology Security Evaluation (notified on 1 September 2009)("CC" hereinafter). It describes the evaluation result and its soundness and conformity.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory Inc. and completed on 22 October 2010. This report grounds on the evaluation technical report (ETR) KSEL had submitted, according to which the TOE has been confirmed to satisfy the CC Part 2 and EAL3+ augmented by ALC_FLR.2 requirements and hence to be ""suitable.""

The TOE, that is a software loaded onto an MFP(multi-function peripheral) providing functions including copy, print, scan and fax feature, performs security functions such as access control on the job MFP is doing, encryption and decryption of user data or TSF data, and image overwriting, etc.



[Figure 1] Operational Environment of the TOE

The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE, and provides identification and authentication of general users and administrators, access control to copy/print/scan/fax job or function offered by MFP, encryption/decryption of the user data or TSF data being stored on HDD, fax data control to block incoming fax data that is not

standardized format of MR, MR, or MH of T.4, network access control to pass or drop network access from the external based on port/protocol, IP address or MAC address, self testing to verify the correct operation of TSF and to examine the integrity of the TSF data and TSF executable code, security audit to generate audit log including job completion, login success/failure or security management, and security management enabling an administrator to manage functions offered by the TOE from RUI or LUI.

Only the authorized administrator is allowed to perform security management using web browsers supporting https protocol, and general users must install printer driver(PCL 6 Driver V3.10.79) or scan manager(Scan Manager V2.00.26) on their remote PC prior to using print or scan function provided by MFP. In addition, external authentication servers(kerberos server, LDAP server or SMB server) to identify and authenticate the general users, external storage servers(FTP server, WebDAV server, SMB server or Mail server) to store fax and scan data transmitted from MFP, and NTP server to synchronize the time of operating system of MFP that is used for generating audit logs should be configured and operated in the operational environment of the TOE.

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

[Table 1] in the below shows the information for identifying TOE.

[Table 1] TOE Identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (No.2009-51 notified by the MOPAS, 1 Sep. 2009) Korea IT Security Evaluation and Certification Scheme (1 Jan. 2010)
Evaluated Product	Samsung MFP Security Kit Type_E V1.0
Protection Profile	N/A
Security Target	Samsung MFP Security Kit Type_E V1.0 Security Target V1.4
Evaluation Technical Report	Evaluation Technical Report of V2.00 of Samsung MFP Security Kit Type_E V1.0
Evaluation Result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V3.1 (No.2009-52 notified by the MOPAS, 1 Sep. 2009)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 Revision 3 (1 Sep. 2009)
Sponsor	Samsung Electronics, Co., Ltd.
Developer	Samsung Electronics, Co., Ltd.
Evaluator	Yongjin Chon, Byongki Park, Injeong Park Korea Security Evaluation Laboratory, Inc.
Certification Body	IT Security Certification Center

The TOE is operated on the four hardware models of MFP(two mono models of SCX-8030/8040, two color models of CLX-9250/9350), detailed hardware specifications are shown in the following [Table 2].

[Table 2] Hardware specification for TOE

Categories				
Features	Mono		Color	
	SCX-8030	SCX-8040	CLX-9250	CLX-9350
Productivity				
CPU	SPGPv4, 800 MHz		PowerPC, 800 MHz	PowerPC, 1.0 GHz
Printing Speed (A4) (Color/Mono)	30ppm/-	40ppm/-	25ppm/ 25ppm	35ppm/ 35ppm
FCOT (Color/Mono)	<7.5 sec / -	<6.5 sec / -	10.5 (color) / <9.5 (mono)	<8.5 (color) / <7.5 (mono)
Warm-up Time (Color/Mono)	< 25 sec / -		< 45 sec	
Duplexing Speed	Same as rated engine speed			
Scanning Speed (A4) (Color)	50ipm @ 300 dpi			60ipm @ 300 dpi
Memory (Standard /Max)	768MB/1.7GB		1GB/2GB	
HDD	250GB			
Image Quality				
Engine Resolution	600 x 600 dpi x 4-bit		600 x 600 dpi x 4-bit	
Resolution Enhancement	4,800 x 600 dpi		4,800 x 600 dpi	
Gradation	256			
Scanning				
Optical Resolution	600 x 600 dpi (Color)			
Scan Resolution Enhancement	4800 x 4800 dpi (Network Scan)			
Output File Type	PDF, TIFF, JPEG, XPS			
Scan-to-Feature	Scan-to-E-mail/FTP/HDD/SMB/I-FAX/URL/LDAP/USB			
Printing				
Max. Imaging Area (mm (inch))	297 x 432 (11.7 x 17)		310 x 452 (12.2 x 18)	
Max. Effective Imaging Area (mm)	297 x 432 (11.7 x 17)		297 x 452 (11.7 x 18)	
Margin2 (LeadingEdge/L-R,mm)	3mm / 2mm		3mm / 2mm	
Emulation	Postscript 3, PCL 6, PDF 1.7+, XPS		Postscript 3, PCL 6, PDF 1.7+, XPS	
Interface	10/100/1000 BaseTX, USB 2.0 3EA			
Supported Operating System	Windows 2000 / XP / 2003 Server / VISTA / 7 /2008 R2, Mac OS 10.5, 10.6, Linux : - Fedora 4 ~ 12 (32/64 bit) - OpenSuSE 10.2, 10.3, 11.0, 11.1, 11.2 (32/64 bit) - SuSE 10.0, 10.1 (32 bit) - Ubuntu 5.04, 5.10, 6.04, 6.10, 7.04, 7.10, 8.04, 8.10, 9.04, 9.10 (32/64 bit) - Mandriva 2005, 2006, 2007, 2007.1, 2008, 2008.1, 2009, 2009.1 (32/64 bit) - Debian 4.0, 5.0 (32/64 bit) - Redhat Enterprise Linux WS 4, 5 (32/64 bit) - SuSE Linux Enterprise Desktop 10, 11 (32/64 bit)			

Faxing		
Resolution	203 x 98, 203 x 196, 203 x 392, 300 x 300, 400 x 400, 600 x 600 dpi	
Data Transmission Speed	33.6kbps	
Communication Mode	Super G3	
Compression Method	JBIG, MMR, MR, MH, JPEG	
Memory	HDD 250G	
Fax-to	Fax-to E-mail/FTP/SMB/HDD	
Media Input		
Standard Tray	520 Sheets x 2 Tray (80 gsm)	
MP Tray	100 Sheets (80 gsm)	
Max. Media Capacity	3,140 Sheets (80 gsm)	
Paper Size - Tray (Min/Max) (mm)	148 x 210 (5.8 x 8.3) / 305 x 457 (12 x 18)	
Paper Size - Bypass (Min/Max) (mm)	89 x 148 (3.5 x 5.8) / 305 x 457 (12 x 18)	89 x 148 (3.5 x 5.8) / 320 x 457 (12.625 x 18)
Paper Size - DADF (Min/Max) (mm)	128 x 128 (5.0 x 5.0) / 297 x 432 (11.7 x 17)	
Paper Weight - Tray (Min/Max)	60 / 163 gsm	60 / 216 gsm
Paper Weight - Bypass (Min/Max)	60 / 216 gsm	60 / 253 gsm
Paper Weight - Simplex ADF (Min/Max)	40 / 163 gsm	
Paper Weight - Duplex ADF (Min/Max)	52 / 135 gsm	
Universal Tray	Tray 1 ~ 4	
Media Output		
Standard Output Capacity	500 (80 gsm)	650 (80gsm)
Max. Output Capacity	650 (80 gsm) (with Inner Output Tray)	650 (80 gsm) (with Right Output Tray)
Output Orientation (Center/Right Tray)	FD/FU	
Sort		
Electronic Sorter	Standard	
Duplex		
Auto Duplex Kit	Standard	
Options		
DADF	Standard	
DCF (Dual Cassette Feeder)	2 Cassette Tray (520 x 2, 80gsm)	
Internal HCF	2,000 (80 gsm, A4, Letter)	
Cabinet Stand	Cabinet Stand	
Job Separator	150 Sheets	N/A
Right Output Tray	N/A	150 Sheets / Standard
1,250-Sheet Standard Finisher	2 Tray (250/1,000 Sheets), 50 Sheets Stapling, 2 Position, Convenience Stapling	
3,250-Sheet Booklet Finisher	2 Tray (250/3,000 Sheets), 50 Sheets Stapling, 15 Sheets Saddle Stiching, 2 Position, Convenience Stapling, 'V' Folding	
Bridge Kit	Connect to Standard Finisher / Booklet Finisher	

Punch Kit	2/3 or 2/4 Holes			
Working Table	Small Side Tablet for Placing a Card Reader			
Keyboard Tray	Keyboard Tray supporting USB Mini-keyboard (US-Only)			
Wireless LAN Kit	802.11 a/b/g			
Fax Kit	Super G3			
Fax Multiline Kit	1 Additional			
Expansion Memory	1GB			
IP Fax Enabler Kit	T.38, SIP			
Common Criteria Security Kit	Advanced Overwrite, Encryption features			
Advanced Scan Kit	OCR, Searchable PDF, Advance Annotations			
SmarThru Workflow	Document Distribution Solution			
CounThru	Accounting Solution			
PM Kit	TBD		Transfer & Clear Kit, Tray Roller Kit, ADF Roller Kit	
Size				
H (with DCF) x W x D (mm)	1154 / 678 / 762			
Weight				
Weight (kg)	107Kg		113kg	
Environment & Regulations				
Environment Regulations	Blue Angel, Energy Star			
Solution Regulations	HIPAA, SOX, FERPA, US Patriot, Section 508, SEC 17a-4			
EME	FCC Class A (US), EU LVD (Europe), VCCI Class A (Japan), CISPR Class A (International, Korea)			
Noise (dB)	TBD		55.9 (Copying), 54.6 (Printing), 39.9 (Stand-by)	
Power (kW)	< 1,500W @ 120V ~ 220V			
Power Savings (Watts)	< 10 W			
Installation Personnel	Service man installation			
Reliability				
Unscheduled Maintenance Rate	10@AMPV 10K		20@AMPV 10K	
Max Monthly Duty	100K	150K	100K	150K
Average Monthly Printing Vol.	8K	12.5K	4K ~ 6K	9K ~ 13K
Toner Yield (Color/Mono)	-/20K	-/35K	12K/15K	20K/25K
OPC Yield (Color/Mono)	-/100K		75K/75K	
Developer Yield (Color/Mono)	-/100K		75K/75K	
Fuser Yield (Color/Mono)	-/150K		150K/150K	
Waste Bottle	75K		75K	
PM Schedule	75K (TBD)		75K	
Machine Life (Max AMPV x 2 x 60 mo)	864,000	1,350,000	720,000	1,560,000
Fault-tolerance	Industry Average			

The four hardware models of MFP that the TOE operates on comprises seven hardware boards, detailed operating system for each hardware board is shown in the following [Table 3]

[Table 3] Operating system for each hardware board

Hardware Board	Operating System	Reference
Main Board	Linux 2.6.29	OS that the TOE is loaded on
GUI Board	Linux 2.6.11	
Scan Board	pSOS	-
Image Converter Board	pSOS	-
Fax Board	pSOS	-
Engine Board	pSOS	-
DADF Board	pSOS	-

System requirements for general user to use print/scan function and administrator to manage the TOE are shown in the following [Table 4].

3. Security Policy

The TOE operates in conformance with the following security policy.

P.USER.AUTHORIZATION

To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.

P.SOFTWARE.VERIFICATION

To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

P.AUDIT.LOGGING

To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be review by authorized personnel.

P.INTERFACE.MANAGEMENT

To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

4. Assumptions and Scope

4.1 Assumptions

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

A.ACCESS.MANAGED

The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

A.USER.TRAINING

TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedures.

A.ADMIN.TRAINING

Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.

A.ADMIN.TRUST

Administrators do not use their privileged access rights for malicious purposes.

A.TIME_STAMP.RELIABLE

The environment of the TOE synchronizes its time with NTP server and provides reliable time-stamps for accurate audit logs about the TOE.

A.OS.TRUST

Administrators remove unnecessary services and means of operating system, and reinforce vulnerabilities upon operating system, and thus ensure reliability and security of the TOE.

A.NETWORK.TRUST

A firewall is installed between internal network and external network to protect the TOE from inward intrusion from outside.

A.SSL.SECURE

SSL protocol protects transferred data between U.USER and the TOE.

A.DBMS.MANAGED

DBMS provides a series of functions including audit log selecting and ordering function, audit log storage protection, and maintenance of audit log integrity.

A.AUTH_SERVER.SECURE

The authentication servers (i.e. LDAP, Kerberos, and SMB Server)

provide a secure remote authentication for U.NORMAL.

A.EXT_SERVER.SECURE

FTP, SMB server, WebDAV, and mail server which store fax and scan data transmitted from the TOE are managed securely.

A.SSL_CERT.INSTALL

Certificate for SSL communication is installed by U.ADMINISTRATOR and the TOE is managed through the secure channel.

A.KEY_GENERATION

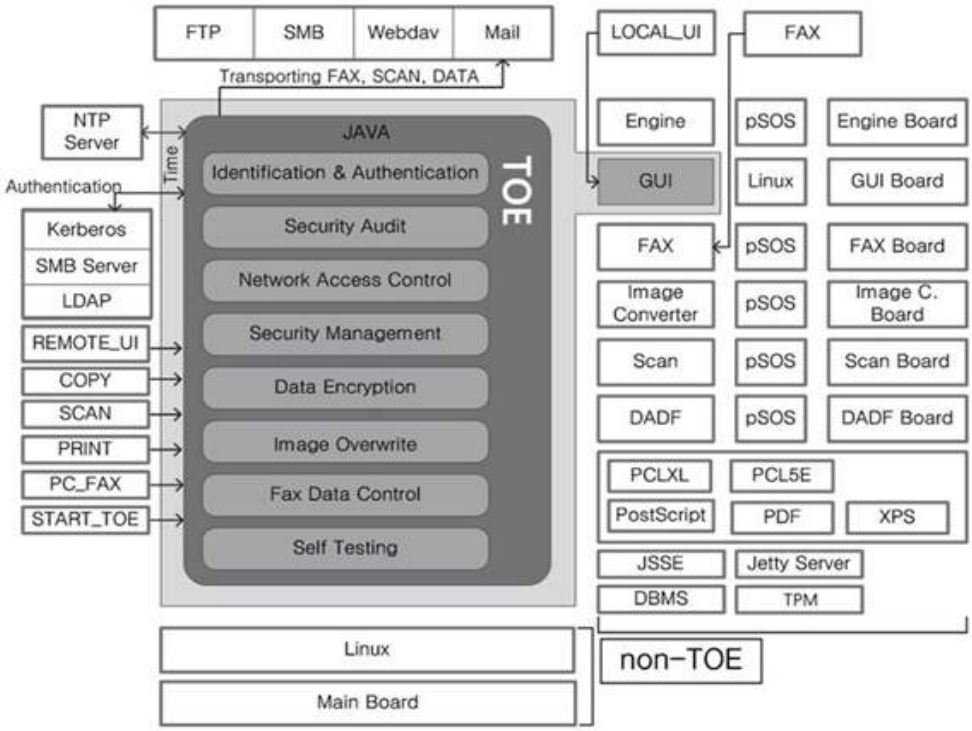
TPM provides cryptographic keys (private key, public key, secure key) to TOE for encryption/decryption of HDD storage data securely.

4.2 Scope to counter a threat

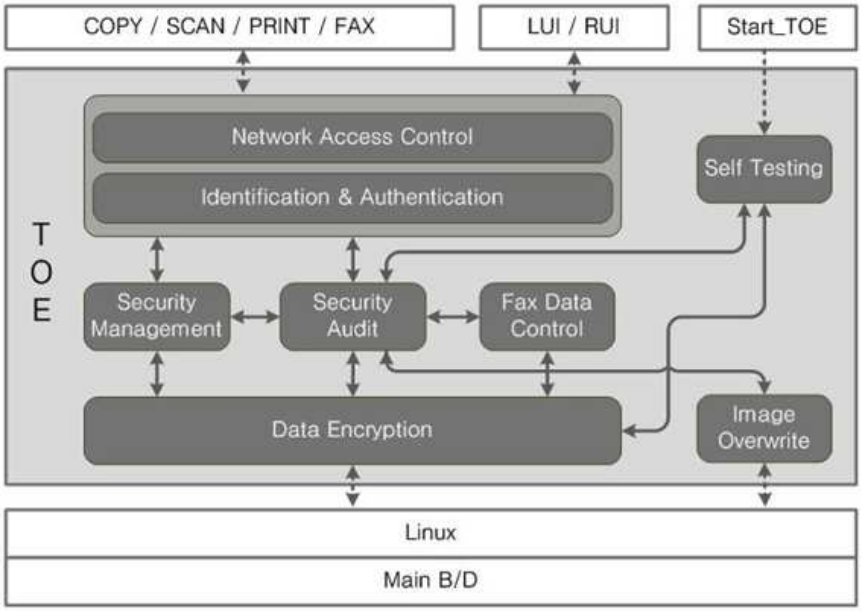
Threat agents are IT entities or users that can adversely access to TOE and the internal asset or harm the internal asset in an abnormal way. The threat agents have basic expertise, resources, and motivation.

5. Product Information

The TOE, that is a software loaded onto an MFP(multi-function peripheral) providing functions including copy, print, scan and fax feature, performs security functions such as access control on the job MFP is doing, encryption and decryption of user data or TSF data, and image overwriting, etc. The physical and logical scope of the TOE are shown in the following [Figure 2], [Figure 3]



[Figure 2] Physical scope of the TOE



[Figure 3] Logical scope of the TOE

The TOE provides the following security functions:

- **Identification & Authentication**

The TOE enforces identification and authentication on the administrator and the general user accessing to the TOE from LUI or RUI. The TOE identifies and authenticates the general users by verifying login information(ID/Password/Domain, Pin Code or ID), or requests external authentication servers(Kerberos server, SMB erver, or LDAP server) for identifying and authenticating the general users instead of the TOE. However, the administrator should be identified and authenticated by entering login information(ID/Password/Domain) only by the TOE. Additionally, the TOE provides the Custom Access Control and TOE Function Access Control based on the user group ID assigned by the authorized administrator when general users perform read, delete, or modify operations on the data owned by them. When the number of consecutive invalid authentication attempts has exceeded the limit number set by the authorized administrator, the account will be locked for certain minutes, and if the user is idle for certain minutes, the mutual session will be terminated automatically.

- **Network Access Control**

The TOE enforces Protocol/Port Control, IP address filtering and Mac address filtering on the network access to the MFP. Protocol/Port Control allows or denies network access by enabling or disabling specific protocols, IP address

filtering allows packets only from IPv4/IPv6 addresses registered by the authorized administrator, On the contrary, MAC address filtering denies packets only from MAC addresses registered by the authorized administrator.

- Security Management

Only the authorized administrator is allowed for security management to modify/add/delete TSF data and security attributes, or enable/disable security functions provided by the TOE from RUI using https protocol or LUI. But, normal user is not allowed to manage security-relevant setting.

- Security Audit

The TOE creates and stores an audit log including job log, security event log and operation log, Only an authorized administrator is allowed to review the audit record through SyncThru Web Service, and when each audit log exceeds the maximum number, the TOE deletes the oldest stored audit records and generates an audit record of deletion. The authorized administrator is able to enable/disable job log and security event log except for operation log.

- Image Overwrite

The TOE provides the image overwriting function on document data, system data, or temporary data produced in the process of print/copy/scan/fax job according to the method defined in Custom, DoD5220.28-M, Australian ASCI 33, or German standard:VSITR. The Image Overwrite function consists of Automatic Image Overwrite enabled to be executed automatically and Manual Image Overwrite executed at the request of the authorized administrator.

- Data Encryption

The TOE provides an encryption function in the process of storing the data(data resulting from print/copy/scan/fax job, configuration information, audit logs) in hard disk drive and a decryption function in the process of accessing stored data from hard disk drive. The TOE requests generating AES Secret key(256bits), that is used during encryption and decryption, to the TPM in the operational environment of the TOE when the TOE is initialized at the first setout, and the TOE performs encryption and decryption of the data using this key. Also, the TOE protects AES Secret key from unauthorized reading and falsification by encrypting the key and storing the encrypted key in the EEPROM, and the TOE destroys cryptographic keys by overwriting a used cryptographic key with a newly generated cryptographic key when the used cryptographic key is altered.

- **Fax Data Control**

The TOE discards fax data if the received fax image is not standardized with MMR, MR, or MH of T.4 specification. And in case that Fax to Email, Fax to FTP, Fax to SMB or Fax to WEBDAV function is enabled, the TOE forwards the received normal fax image to external storage server(mail server, FTP server, SMB server, or WebDAV server).

- **Self Testing**

The TOE carries out self testing at initial booting of MFP to ensure the correct operation of data encryption function(TSF_NVE). And the TOE verifies the integrity of TSF executable code(TSF_NVE) and TSF data(Encryption key) to provide self-protection.

6. Guidance

The TOE provides the following guidance documents:

- CLX-9250 9350 Series Multi-Functional Printer Administrator's Guide REV. 1.06 (2010.08.25)
- CLX-9250 9350 Series Color Multi-Functional Printer User's Guide REV. 1.04 (2010.03.30)
- SCX-8030 8040 Series Multi-Functional Printer Administrator's Guide REV. 1.03 (2010.08.25)
- SCX-8030 8040 Series Multi-Functional Printer User's Guide REV. 1.02 (2010.08.25)
- CLX-9250 9350 Series Installation Guide V300 (2010.08.25)
- SCX-8030 8040 Series Installation Guide V101 (2010.08.25)

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 described in the test document 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, internal and external network. Also, it describes 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**

Test document describes 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.

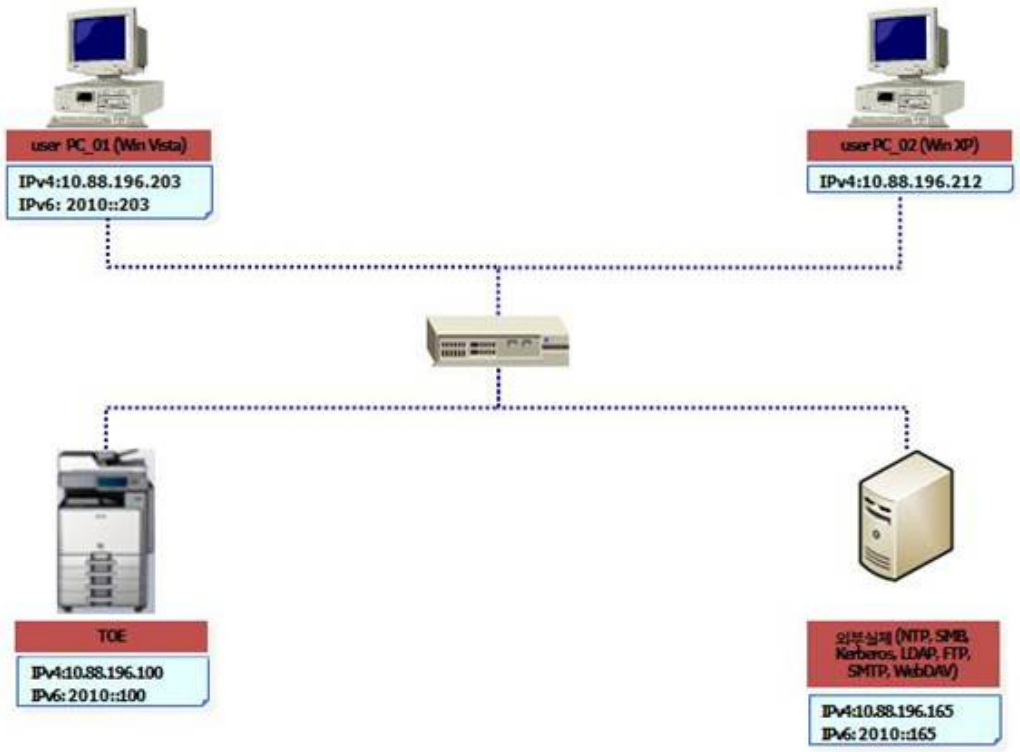
The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

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

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



[Figure 4] Evaluator's test configuration

9. Evaluation Result

The evaluation applied the Common Criteria and the Common Methodology for Information Technology Security Evaluation V3.1 Revision 3. It concludes that the TOE satisfies the CC V3.1 part 2 and EAL3+ of the CC V3.1 part 3. The detailed information regarding the evaluation is described in the ETR.

- **ST Evaluation (ASE)**

The ST introduction contains ST reference, TOE reference, TOE overview and TOE description. ST reference uniquely identifies the ST, and TOE reference identifies the TOE and TOE reference is not misleading. TOE overview describes the usage or major security features of the TOE and any non-TOE hardware/software/firmware required by the TOE, and TOE description describes physical and logical scope of the TOE.

Conformance claim identifies the version of the CC to which the ST and the TOE claim conformance. The CC conformance claim describes the conformance of the ST to CC Part 2 conformant and CC Part 3 conformant. Also, the conformance claim describes any conformance of the ST to a package as package-conformant.

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.

The security objectives describe the security objectives of the TOE and the operational environment of the TOE, and the security objectives rationale demonstrates that the security objectives counter all threats, enforce all OSPs, and uphold all assumptions.

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined, and each dependency of the security requirements is either be satisfied, or the security requirements rationale justifies the dependency is not being satisfied. Also, the security requirements rationale traces each SFR back to the security objectives for the TOE and explains why the SARs were chosen.

The TOE summary specification describes how the TOE meets each SFR.

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

• Development Evaluation (ADV)

The functional specification describes the purpose, method of use, all parameters, all actions and direct error messages resulting from invocation of the TSFI.

The TOE design describes the structure of the TOE in terms of subsystems and provides a description of the interactions among all subsystems of the TSF.

The security architecture is described at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document. And it describes how the TSF initialisation process is secure, and demonstrate that the TSF protects itself from tampering and the TSF prevents bypass of the SFR-enforcing functionality. Also, it describes the security domains maintained by the TSF.

Therefore, a functional specification describing TSFI, a TOE design describing the architecture of the TOE in terms of subsystems and a security architecture description are suitable for use as the basis for the TOE evaluation.

• Life Cycle Support Evaluation (ALC)

CM capabilities provides the TOE label for its unique reference, uniquely identifies all configuration items and describes the method used to uniquely identify the configuration items. It provides the measures such that only authorized changes are made to the configuration items and describes how the CM system is used for the development of the TOE. Also, CM scope includes the TOE, the evaluation evidence required by the SARs, the parts that comprise the TOE and the implementation representation, and it indicates the developer of the TSF relevant configuration items.

The delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

The development security documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

The life-cycle definition documentation describes the model used to develop and maintain the TOE and the necessary control over the development and maintenance of the TOE.

Flaw reporting procedures describe the procedures used to track all reported security flaws by developers, identifies corrections and guidance on corrective actions, and describes the procedures of delivering the remediation procedures to TOE users.

Therefore, the life-cycle support describes CM procedures, delivery procedures, security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation, the model used to develop and maintain the TOE and Flaw reporting procedures, and hence it is suitable for use as the basis for the TOE evaluation.

• Guidance Documents Evaluation (AGD)

Operational user guidance describes, for each user role, how to use the available interfaces provided by the TOE in a secure manner, and Preparative procedures describes all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

Therefore, the user guidance documents describing how to use the TOE and preparative procedures describing all the steps necessary for secure acceptance and installation of the delivered TOE are described adequately, and hence these are suitable for use as the basis for the TOE evaluation.

• Tests Evaluation (ATE)

The tests have been sufficient to establish that TSFIs in the functional specification, TSF subsystems and SFR-enforcing modules in the TOE design had been systematically tested.

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 hence these are suitable for use as the basis for the TOE evaluation.

• Vulnerability Assessment Evaluation (AVA)

The evaluator has searched for potentially exploitable vulnerabilities based upon analysis of the evaluation evidence(such as security target, functional

specification, TOE design and security architecture description) and a search of publicly available material.

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

The user installing and operating the TOE must obey the following recommendations.

- SSL protocol in the operational environment of the TOE protects transmitted data between SyncThru Web Service(web browser) and the TOE, and the TOE provides a function generating certificate itself for this SSL protocol. Therefore, administrator should access and manage the TOE using https protocol after generating certificate for SSL communication in case of starting the TOE at the first time.

- If there are any problems, such as blackout or power failure, during manual image overwriting, the image overwriting job is terminated yet the image overwriting on the memory area has remained uncompleted. But authorized administrator must keep in mind that the manual image overwriting job automatically restarts to overwrite the remaining area if the power button is pushed again.

- There are two types of users, administrators(role of admin) allowed to manage the TOE and general users(role of general user, restricted info. user, limited resource user, guest) allowed to use the function of MFP such as print, copy, scan, fax, and etc. Therefore, authorized administrator must be careful not to grant the role of admin to general users only given the rights to use print, copy, scan or fax function of MFP.

11. Acronyms and Glossary

The following terms are used in this report:

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

LUI (Local User Interface)	Interface for general users or system administrators to access, use, or manage the MFP directly
RUI (Remote User Interface)	Interface for general users or system administrators to access, use, or manage the MFP through a web service
MFP (Multi-Function Peripheral)	MFP is a machine that incorporates the functionality of multiple devices (copy, print, scan, or fax) in one
TPM (Trusted Platform Module)	Trusted Platform Module offers facilities for the secure generation of cryptographic keys - often called the "TPM chip" or "TPM Security Device"
DoD 5200.28-M	DoD 5200.28-M is an image overwriting standard that Department of Defense recommends. The image data in a storage device is completely overwritten three times with overwriting '0x35' the first time, then '0xCA' the second time, and finally overwriting '0x97'
Australlian ASCI 33	The Australian Government Information and Communications Technology Security Manual (also known as ACSI 33) has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on how to protect their Information Technology, and Communications systems
VSITR	The German Federal office for IT Security released the VSITR standard, which overwrites the hard drive with 7 passes. For the first 6 passes, each overwrite reverses the bit pattern of the previous pass, inverting the bits in order to destabilize the remnants of data that may exist on the edges of the track of the disk to which the data is written. The final pass

	amplifies the effect, overwriting the entire disk with "01010101"
T.4	Data compression specification for fax transmissions by ITU-T
MH	Abbreviation of Modified Huffman coding. This is an encoding method to compress for storing TIFF type files. It is mainly used for fax transmission
MR	Abbreviation of Modified Relative Element Address Designate MH coding
MMR	Abbreviation of Modified Modified Relative Element Address Designate MH coding. More advanced type than MR coding

12. Reference

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

[1] Common Criteria for Information Technology Security Evaluation (Sep. 2009)
[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_E V1.0 Security Target Version 1.4 (23 Aug. 2010)
[6] Evaluation Technical Report of V2.00 of Samsung MFP Security Kit Type_E V1.0 (2010. 10. 22)