KECS-CR-12-09

Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 Certification Report

Certification No.: KECS-CISS-0365-2012

2012. 1. 25

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2012.1.25	-	Certification report for Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 - First documentation

This document is the certification report for Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 of Samsung Electronics.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL3+ evaluation of Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 from Samsung Electronics Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is an embedded software product for MFPs (Multi-Function Peripherals) as an IT product. It controls the operation of the entire MFP, including copy, print, scan, and fax functions on the MFP controller.

The MFP can be used in a wide variety of environments, which means each environment may place a different value on the assets, make different assumptions about security-relevant factors, face threats of differing approaches, and be subject to different policy requirements.

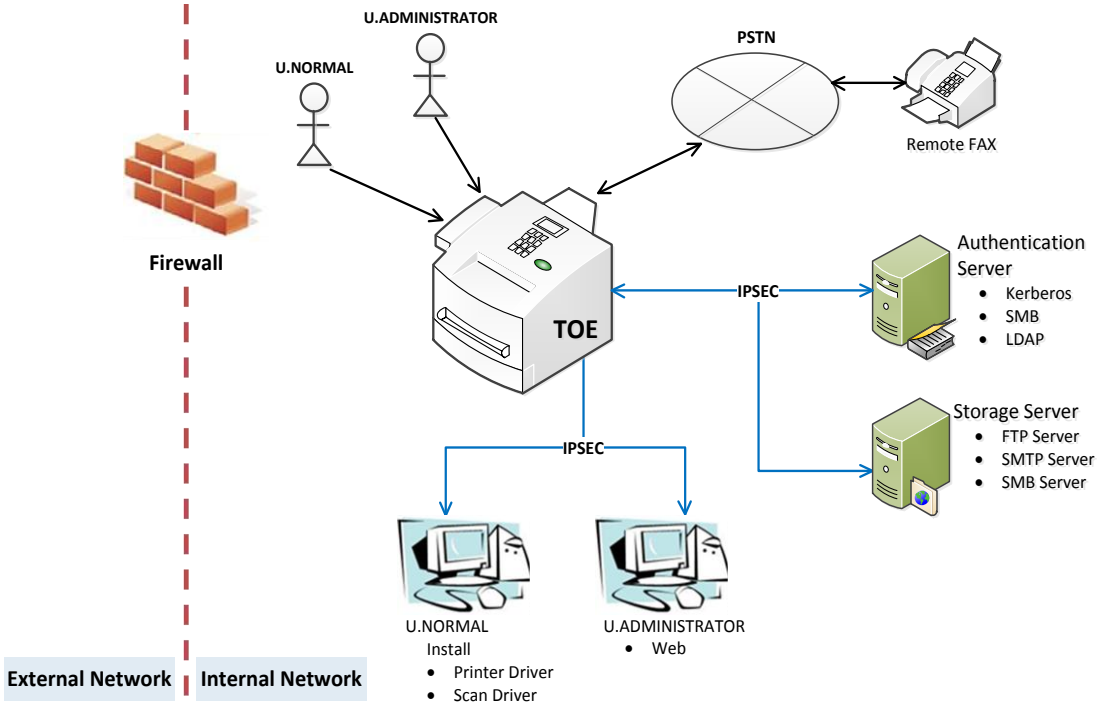
The TOE Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 composed of the following components:

- Embedded control software V2.0.0.03.00 provided by Samsung Electronics.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on December 27, 2011. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [5] and the Security Target (ST) [6].

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL3 augmented by ALC_FLR.2. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

The TOE is operated in an internal network protected by a firewall. User is connected to the TOE and may perform jobs that are allowed. The TOE is intended to operate in a network environment that is protected by a firewall from external malicious attacks (e.g., DoS attack), and with reliable PCs and authenticated servers. A user is able to access the TOE by using a local user interface, PC from a remote user, or a Remote User Interface, as shown below.



[Figure 1] TOE Operational Environment

The local user interface (LUI) is designed to be accessed by users and a local administrator. The users can operate copy, scan, and fax functions through the LUI. In the case of a scanning job, users can operate the scanning job using the LUI and transfer the scanned data to a certain destination by email addresses, server PCs, or client PCs. Users can also use their PCs to print out documents or to access the TOE through the internal network. The administrator can enable/disable Automatic Image Overwrite, start/stop Manual Image Overwrite, and change a Password via the LUI. The administrator can access the TOE through the Remote User Interface (WEBUI) using a web browser supporting SSL protocol. From there, they can add/change/delete user accounts, change the web administrator's ID and password, enable/disable the security audit service, and download the security audit report. The user account information that requires asking for internal authentication by TOE (only for network-scan services such as scan manager, scan to e-mail, scan to FTP, scan to SMB) can be stored on the hard disk drive of the MFP. All of the information stored on the hard disk drive is protected by the TOE. In the case of external authentication by trusted authentication servers (Kerberos, LDAP, SMB server), all the account information stored on a network authentication server is assumed to be protected from external environmental space.

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is product package consisting of the following components and related guidance documents.

Type	Identifier	Release	Delivery Form
SW	CLX-8385NX/8540NX Control Software	1.15.00.07	MFP (Note: The SW is contained in ROM and EEPROM)
	SCX-5835NX Control Software	2.00.01.12	
	SCX-6555NX Control Software	2.00.02.32	
	SCX-6545NX Control Software	2.00.02.34	
DOC	CLX-8385NX/8540NX User Guide	v1.02	Softcopy
	SCX-5835NX User Guide	v1.01	
	SCX-6555NX User Guide	v1.04	
	SCX-6545NX User Guide	v1.03	

[Table 1] TOE identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009) Korea Evaluation and Certification Regulation for IT Security (July 20, 2011)
TOE	Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~

	CCMB-2009-07-003, July 2009
EAL	EAL3+(augmented by ALC_FLR.2)
Protection Profile	IEEE Std 2600.1-2009 Version 1.0
Developer	Samsung Electronics Co., Ltd.
Sponsor	Samsung Electronics Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	December 27, 2011
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [6] by security objectives and security requirements. The TOE provides security features to identify and authenticate authorized users, to generate audit records of the auditable events, and to securely manage the TOE functionality and authorized user accounts information.
For more details refer to the ST [6].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [6], chapter 3.3):

- 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.
- TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedures.
- 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 to correctly configure and operate the TOE in

accordance with those policies and procedures.

- Administrators do not use their privileged access rights for malicious purposes.
- A firewall is installed between the internal network and the external network to protect the TOE from intrusion from outside.
- The authentication servers (i.e. LDAP, Kerberos, and SMB Server) provide a secure remote authentication for U.NORMAL.
- The FTP, SMB server, and mail servers that store fax and scan data transmitted from the TOE are managed securely.
- Certificate for SSL communication is installed by U.ADMINISTRATOR and the TOE is managed through the secure channel.
- All of the external servers(Storage, Authentication Server) that connected with the TOE via network supports IPSEC.
- All of the client PCs that connected with the TOE via network supports SSL.

It is assumed that the TOE is installed and operated based on the following hardware and operating system.

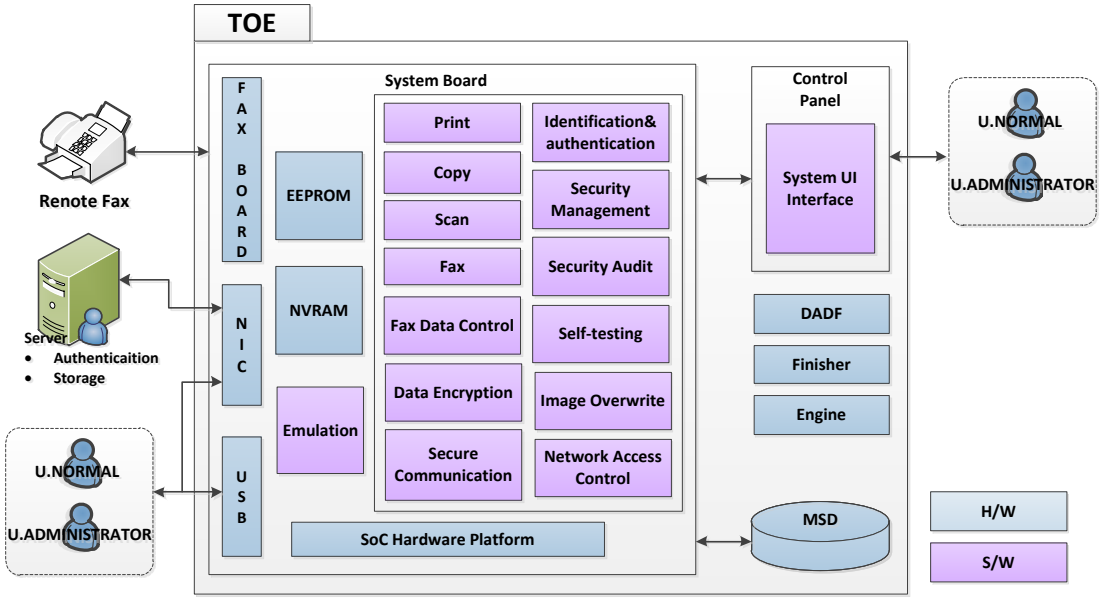
Specifications		**SCX-5835NX**	**SCX-6545NX**	**SCX-6555NX**	**CLX-8385NX** **CLX-8540NX**
LCD		800x480 7" WVGA Color Touch-Screen LCD	800x480 7" WVGA Color Touch-Screen LCD	800x480 7" WVGA Color Touch-Screen LCD	800x480 7" WVGA Color Touch-Screen LCD
CPU		Chorus3 (360 MHz)	Orion(600 MHz)	Orion(600 MHz)	SPGPv4 (800 MHz)
System Memory		256 MB	256 MB	256 MB	256 MB
HDD		160 GB HDD	160 GB HDD	160 GB HDD	160 GB HDD
SD Card		2 GB	2 GB	2 GB	2 GB
FAX	Compatibility	ITU-T G3, Super G3	ITU-T G3, Super G3	ITU-T G3, Super G3	ITU-T G3, Super G3
	Comm. System	PSTN / PABX	PSTN / PABX	PSTN / PABX	PSTN / PABX
	Modem Speed	33.6 Kbps	33.6 Kbps	33.6 Kbps	33.6 Kbps
Interface		Hi-Speed USB 2.0, Ethernet 10/100/1000 base	Hi-Speed USB 2.0, Ethernet 10/100/1000 base	Hi-Speed USB 2.0, Ethernet 10/100/1000 base	Hi-Speed USB 2.0, Ethernet 10/100/1000 base

	TX, USB host 2.0	TX, USB host 2.0	TX, USB host 2.0	TX, USB host 2.0
Extra Information	Simplex :Up to 33 ppm in A4 (35 ppm in Letter)	Simplex :Up to 43 ppm in A4 (45 ppm in Letter)	Simplex :Up to 53 ppm in A4 (55 ppm in Letter)	B&W: Up to 38 ppm in A4 (40 ppm in Letter) Color: Up to 38 ppm in A4 (40 ppm in Letter)
OS	pSOS 2.5			VxWorks 6.6
Database	H2 DB 1.2.142			

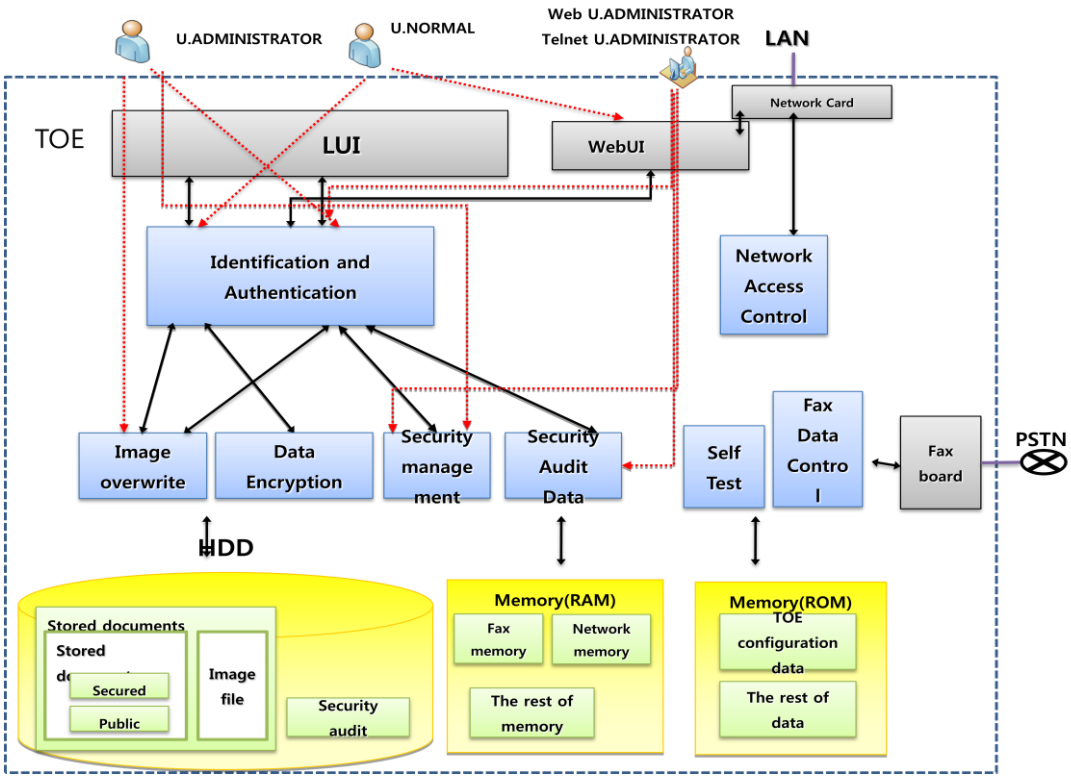
[Table 3] Required non-TOE Hardware and OS

5. Architectural Information

[Figure 4] and [Figure 5] show architectural information and the logical scope of the TOE.



[Figure 2] Architectural Information of the TOE



[Figure 3] Logical boundary of the TOE

- Identification & Authentication

The TOE receives user's information (e.g. ID, password, domain, etc.) through either the LUI or the WEBUI, and performs identification & authentication functions using the acquired information. Then the TOE authorizes user according to the identification & authentication result. The TOE also provides the Common Access Control & TOE Function Access Control based on the user role assigned to user ID by administrator.

- Network Access Control

The TOE provides a network access control function to control ports and protocols used in network protocol services provided by the MFP. Through this function, administrator can control access from external network by enabling/disabling or altering port numbers of various protocols. And the TOE also provides IP filtering /Mac filtering functions to control access from external network.

- Security Management

The TOE provides a management function to manage security functions (e.g. security audit, image overwrite, etc.) provided by the TOE. Through this function, administrator can enable/disable security functions, manage TSF data and the security attributes,

and maintain security roles.

- Security Audit

The TOE stores and manages internal events occurring in the MFP. Audit logs are stored on the hard disk drive and can be reviewed or deleted or exported by administrator through the remote user interface.

- Image Overwrite

The TOE provides an image overwrite function to securely delete temporary files and job files (e.g. printing, copying, scanning, and faxing jobs). This function is classified as two functions: automatic image overwriting and manual image overwriting. An Administrator can execute the image overwriting function only through the local user interface.

- Data Encryption

The TOE provides a data encryption function to protect data (e.g. job information, configuration information, audit logs, etc.) stored on the hard disk drive from unauthorized access.

- Fax Data Control

The TOE provides a fax data control function to examine fax image data formats (MMR, MR, or MH of T.4 specification) received via the PSTN port and check whether received data is suitable.

- Self-testing

The TOE provides a self-testing function to verify the TSF's correct operation and the integrity of TSF data and executable code.

- Secure Communication

The TOE provides a trusted channel between itself and another trusted IT product to protect user data or TSF data that are transmitted or received over network.

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
CLX-8385NX/8540NX User Guide	v1.02	October 14, 2011
SCX-5835NX User Guide	v1.01	October 14, 2011

Identifier	Release	Date
SCX-6555NX User Guide	v1.04	October 14, 2011
SCX-6545NX User Guide	v1.03	October 14, 2011

[Table 4] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. The developer's tests were performed on each distinct operational environment of the TOE (see chapter 1 of this report for details about operational environment of the TOE).

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined in the functional specification, and demonstrated that the TSF behaves as described in the functional specification.

The developer tested subsystems including their interactions, and analyzed testing results according to the assurance component ATE_DPT.1.

Therefore the developer tested all SFRs defined in the ST [6].

The evaluator performed all the developer's tests (a total of 112 tests), and conducted a total of 32 independent testing based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [7]. The evaluator considered followings when devising a test subset:

- TOE security functionality: The TOE is an embedded software product for MFPs (Multi-Function Peripherals) as an IT product. It controls the operation of the entire MFP, including copy, print, scan, and fax functions on the MFP controller, and
- Developer's testing evidence: The evaluator analyzed evaluation deliverables for ATE_COV.2, ATE_DPT.1, and ATE_FUN.1 to understand behavior of the TOE security functionality and to select the subset of the interfaces to be tested, and
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL3+, and the evaluator tried to balance time and effort of evaluator's activities between EAL3+ assurance components.

Also, the evaluator conducted a total of 18 penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, weak cryptography, flaws in networking protocol implementation, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00. The TOE is an embedded software product for MFPs as an IT product. It controls the operation of the entire MFP, including copy, print, scan, and fax functions on the MFP controller.

The TOE is identified by TOE name and version number including release number. The TOE identification information is provided GUI.

And the guidance documents listed in this report chapter 6, [Table 3] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL3+.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE

description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The ST doesn't define any extended component. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer uses a CM system that uniquely identifies all configuration items, and the ability to modify these items is properly controlled. Therefore the verdict PASS is assigned to ALC_CMC.3.

The configuration list includes the TOE, the parts that comprise the TOE, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.3.

The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Therefore

the verdict PASS is assigned to ALC_DVS.1.
The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.
The evaluator shall examine the flaw remediation documentation provided to determine that discovered security flaws be tracked and corrected by the developer. Therefore the verdict PASS is assigned to ALC_FLR.2
Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, and the delivery activity.
The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.
The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. It provides a detailed description of the SFR-enforcing subsystems and enough information about the SFR-supporting and SFR-non-interfering subsystems for the evaluator to determine that the SFRs are completely and accurately implemented. Therefore the verdict PASS is assigned to ADV_TDS.2.

The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, the actions, results and error messages of each TSFI are also described sufficiently that it can be determined whether they are SFR-enforcing, with the SFR-enforcing TSFI being described in more detail than other TSFIs. Therefore the verdict PASS is assigned to ADV_FSP.3.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), and a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.

The developer has tested the TSF subsystems against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.1.

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing Basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.2.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing Basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_CMS.3	ALC_CMS.4.1E	PASS	PASS	
	ALC_CMC.3	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.1	ALC_DVS.1.1E	PASS	PASS	
		ALC_DVS.1.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
	ALC_FLR.2	ALC_FLR.2.1.E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.2	ADV_TDS.2.1E	PASS	PASS	PASS
		ADV_TDS.2.2E	PASS	PASS	
	ADV_FSP.3	ADV_FSP.3.1E	PASS	PASS	
		ADV_FSP.3.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.1	ATE_DPT.1.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- Since the image overwrite can only be done manually, the administrator of the TOE should perform it regularly to protect user data.
- Since the audit data storage is overwritten by the image overwrite, make sure that the audit data is exported for backup before launching the image overwrite function.
- A system administrator should enable the IPSec provided by the TOE for a

safe communication between the TOE and IT entities such as a system administrator's PC, general user's PC, and authentication server; and set up the IPSec for IT entities.

- An administrator is recommended to enable the alarm for an authentication failure of a secure print user so that it can be taken care of immediately.
- The TOE is delivered with the default password of the 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.
- Use the TOE function to configure allowed administrator's IP's so that unauthorized access can be blocked.

11. Security Target

The Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 Security Target v1.3, October 14, 2011 [6] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RFC	Request For Comments
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Functionality
Multi-Function Printer, MFP	MFP is a machine that incorporates the functionality of multiple devices (copy, print, scan, or fax) in one.
LUI, Local User Interface	An interface for a system administrator and a general user to access, use, or manage the TOE directly.
Web UI, Web User Interface	An interface for a system administrator and a general user to access, use, or manage the TOE through a web service.
Image Overwrite	A function to delete all stored files on the hard disk drive. The image data is overwritten three times by using DoD 5200.28-M standard. The TOE provides Manual Image Overwrite function.
Manual Image Overwrite	Only an authorized local administrator can invoke this feature. Once invoked, the Manual Image Overwrite overwrites all stored files, including image files and preserved files.
Image file	Temporary files of user data that are stored on the MSD in a format that the TOE can process during a scan, copy, or fax job.
Preserved file	Files stored on the MSD by a user in a format of electronic image file. There are two types to store a file on the MSD: 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, the user must set a PIN required to access the file. Then the file can only be accessed by entering the PIN.
Stored file	Every stored file on the MSD. It includes preserved files and temporary files(image files)
Secure print	When a user stores a file in an MFP from a remote client PC, the user must set security printing configuration and assign a PIN on the file. Then the user can access the file by entering the PIN through the LUI of the MFP,

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-004, July 2009

[3] Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009)

[4] Korea Evaluation and Certification Regulation for IT Security (July 20, 2011)

[5] Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 Evaluation Technical Report V2.0, December 27, 2011

[6] Samsung SCX-5835NX SCX-6555NX SCX-6545NX CLX-8385NX CLX-8540NX Control Software V2.0.0.03.00 Security Target v1.3, October 14, 2011