KECS-CR-17-22

Sindoh MF2000, MF3000, MF4000, N610, N410 Series

Certification Report

Certification No.: KECS-CISS-0786-2017

2017. 4. 21

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2017.4.21	-	Certification report for Sindoh MF2000, MF3000, MF4000, N610, N410 Series - First documentation

This document is the certification report for Sindoh MF2000, MF3000, MF4000, N610, N410 Series of Sindoh Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory (KSEL)

Table of Contents

1. Executive Summary

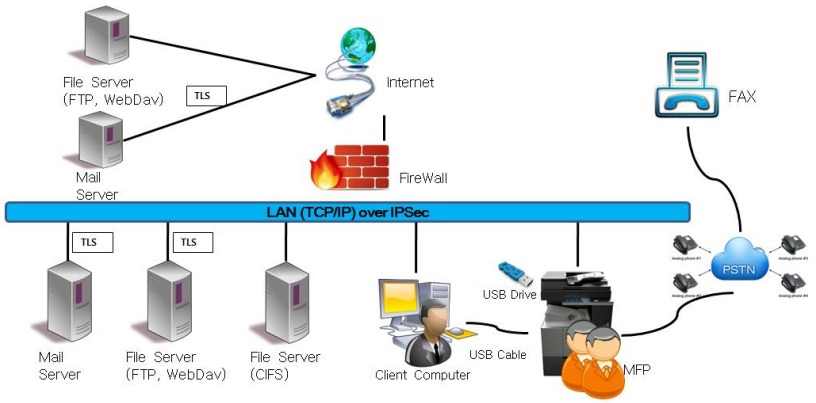
This report describes the certification result drawn by the certification body on the results of the EAL2 evaluation of Sindoh MF2000, MF3000, MF4000, N610, N410 Series from Sindoh Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is 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 evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on April 4, 2017. This report grounds on the evaluation technical report (ETR) KSEL had submitted and the Security Target (ST) [4]. 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 EAL2. Therefore the ST and the resulting TOE is CC Part 3 conformant.

The Security Functional Requirements (SFRs) are based upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. The statement of security requirements identify the extended security requirement. The extended SFR component (FPT_FDI_EXP Restricted forwarding of data to external interfaces) has been clearly and unambiguously defined, and whether it is necessary. Therefore the ST and the resulting TOE is CC Part 2 extended.

The TOE is operated in an internal network protected by a firewall. U.USER is connected to the TOE and may perform jobs that are allowed (see Figure 1).



[Figure 1] TOE Operational Environment

The TOE is intended to operate in a network environment that is protected by a firewall from external malicious attacks, and with reliable PCs and authenticated servers. U.USER is able to access the TOE by using local user interface (LUI) or remote user interface (RUI). The LUI is designed to be accessed by U.USER. The U.NORMAL can operate copy, scan, and fax functions through the LUI. In the case of a scanning job, U.USER can operate the scanning job using the LUI and transfer the scanned data to a certain destination by email addresses and servers. U.NORMAL can also use their PCs to print out documents or to access the TOE through the internal network. U.ADMINISTRATOR can manage security features like format/delete SD card and SSD, and change a Password via the LUI. U.ADMINISTRATOR can access TOE through the RUI using a web browser through IPSec protocol. If IPSec is not configured in the TOE, all of network connection would be blocked. From there, U.ADMINISTRATOR can add/change/delete user accounts, change the U.ADMINISTRATOR's ID and password, review the security audit service. The U.USER's account information that requires asking for internal authentication by TOE can be stored on NAND Flash of the TOE. All of the information stored on the NAND Flash is protected by the TOE.

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 identified using TOE name, S/W Package and Components as follows:

Developer	Sindoh Co., Ltd.
TOE Name	Sindoh MF2000, MF3000, MF4000, N610, N410 Series
S/W Package	JUNIPER_Pkg_170327_2 (JUNIPER_Pkg_170327_2.zip)
Components	JUNIPER_CTL : JUNIPER_170327_2 JUNIPER_S_EGB : 02.06.41 JUNIPER_S_UICC : 0.0.8 JUNIPER_S_DFC : 01.59 JUNIPER_BANK : 1.02 JUNIPER_C_EGB : 02.06.40 JUNIPER_C_UICC : 0.0.8 JUNIPER_C_DFC : 01.45
MFP Models	MF2083, MF3033, MF4041, MF4091, N610, N611, N612, N613, N410, N411

[Table 1] TOE identification

The firmware and software included in the TOE are identified as follows:

Classification	N410, N411	N610, N611, N612, N613, MF2083, MF3033, MF4041, MF4091
Controller S/W	JUNIPER_CTL :JUNIPER_170327_2	
Engine Control F/W	JUNIPER_C_EGB :02.06.40	JUNIPER_S_EGB :02.06.41
UICC Control F/W	JUNIPER_C_UICC :0.0.8	JUNIPER_S_UICC :0.0.8
DFC Control F/W	JUNIPER_C_DFC :01.45	JUNIPER_S_DFC :01.59
Tray Control F/W	JUNIPER_BANK :1.02	

[Table 2] Firmware and software included in the TOE

Scheme	Korea Evaluation and Certification Guidelines for IT Security (June 27, 2016) Korea Evaluation and Certification Regulation for IT Security (November 1, 2012)
TOE	Sindoh MF2000, MF3000, MF4000, N610, N410 Series
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL2
Protection Profile	ST does not claim conformance to PP
Developer	Sindoh Co., Ltd.
Sponsor	Sindoh Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	April 4, 2017
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

[Table 4] shows the specification for TOE.

MFP Model		**N410**	**N411**	**N610**	**N611**	**N612**	**N613**	**MF2083**	**MF3033**	**MF4041**	**MF4091**
Specification											
Copy speed (unit: ppm)		26	30	26	30	40	45	26	30	40	45
Memory(RAM)		1GB		2GB							
Scanner Type		CIS		CCDM							
Duplex		Standard									
OP Type		5 inch Color TFT LCD		9 inch Color TFT LCD							
CPU		Quad Core (800MHz Dual Core + 533MHz Dual Core)									
FAX module		Standard									
Storage	SD Card	(None) or 32GB		(None) or 64GB				32GB			
	SSD	(None) or 256GB		(None) or 256GB				(None) or 256GB			
	Nand Flash	512MB		512MB				512MB			
PS/PCL Control		Standard (PCL 6, PCL5e, PS3)									

[Table 4] General Specification for TOE

3. Security Policy

The TOE complies security policies defined in the ST [4] 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 [4].

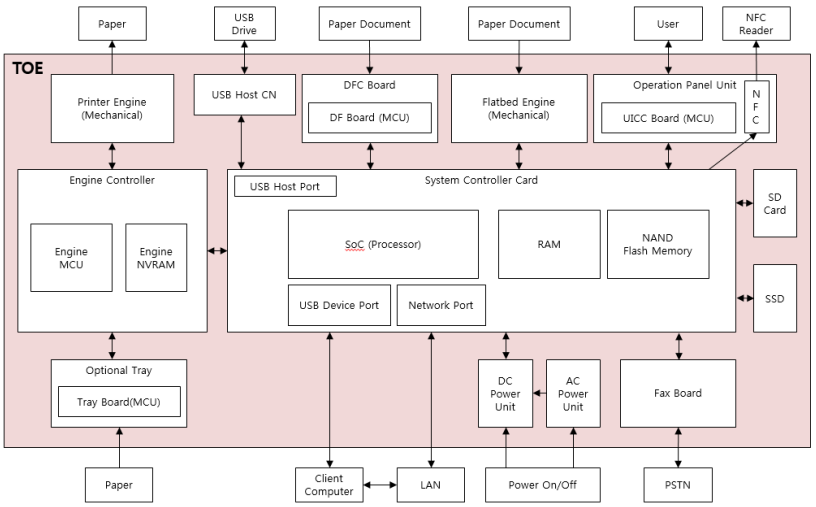
4. Assumptions and Clarification of Scope

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 [4], chapter 3.3):

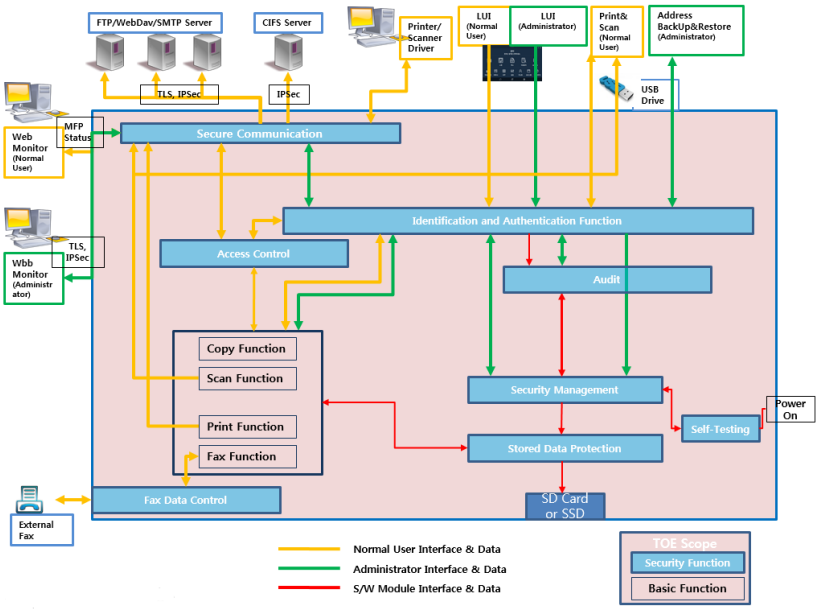
- The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
- TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies 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 correctly configure and operate the TOE in accordance with those policies and procedures.
- Administrators do not use their privileged access rights for malicious purposes.

5. Architectural Information

[Figure 2] and [Figure 3] show the scope of the TOE.



[Figure 2] Physical Structure of MFP



[Figure 3] Logical boundary of the TOE

- Identification and Authentication

  To be able to access the TOE (using LUI or RUI) and use its functions, users must be identified and authenticated using their ID/password. The identification and authentication data of a user is stored in the database inside the TOE. When a user makes authentication errors for the number of consecutive times pre-defined by the administrator, the authentication will be limited according to the following authentication policies.

  Administrator: Authentication is delayed for a specified amount of time

Normal user: Authentication is prevented until it is re-allowed by the administrator

Normal users can be identified and authenticated only through LUI, and the administrator can be identified and authenticated through both LUI and RUI.

- Access Control

  The TOE controls users who can access the document data generated by the print, scan, fax and copy function based on the user ID, and denies all accesses except for document owners. According to the basic function access right set by the administrator, the execution rights are controlled based on user ID and user role. All accesses of normal users except the ones explicitly permitted by the administrator are denied. The TOE provides the function to deny all accesses except for the IPs allowed by the administrator.

- Audit

  The TOE stores and manages internal history of actions occurring in the TOE, such as the MFP job log, fax log, and audit log. These logs can be viewed and managed only by the administrator through the operation panel. The job log (Print, Scan and Copy) and the fax log (Fax) can be viewed by the administrator and normal users.

- Security Management

  The TOE provides Security Management functions for managing TSF data and security attributes (e.g. management of audit records, user management, IP filtering function management, and user data repository management) necessary for safely managing the TOE. Security management functions can be performed only by the administrator through LUI or RUI.

- Stored Data Protection

  Temporal save data for printing/fax transmission and permanent archive data are stored in the user data repository (SD Card or SSD) installed in the TOE. To protect the user data stored in the data repository, the function to encrypt the data repository is provided. Also, the function to delete the data stored in the data repository is provided to prevent user data in the data repository from leaking out.

- Self-Testing

  To demonstrate correct operation of the TSF, the TOE conducts self-tests at during start-up, periodically during normal operation, at the request of the authorized users. It also provides the function to verify the integrity of TSF data and TSF to authorized users to assure that the TSF is operating correctly.

- Fax Data Control

  Unless explicitly permitted by the authorized administrative role, the forwarding of inbound fax data through PSTN to external interfaces is limited by the TOE. Except for the fax data, the forwarding of the data received from all external interfaces to all other external interfaces is also limited.

- Secure Communication

  The TOE provides an encrypted communication channel for the communication between TOE and external IT entity to protect user data or TSF data transmitted.

External IT Entities	Encrypted Communication Protocols
Client Computer	IPSec, TLS
FTP server	IPSec, TLS
WebDAV server	IPSec, TLS
Mail server	IPSec, TLS
CIFS server	IPSec

6. Documentation

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

Identifier	Version
Sindoh MF2000, MF3000, MF4000, N610, N410 Series User Manual (N410/MF Series)	V1.8
Sindoh MF2000, MF3000, MF4000, N610, N410 Series User Manual (N610/MF Series)	V1.8

[Table 5] 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.1. 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.

Therefore the developer tested all SFRs defined in the ST [4].

The evaluator performed all the developer's tests, and conducted independent testing listed in ETR [3], based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [4]. The evaluator considered followings when devising a test subset:

- TOE security functionality: The TOE is 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.1, ATE_FUN.1, and ATE_IND.2 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 EAL2, and the evaluator tried to balance time and effort of evaluator's activities between EAL2 assurance components.

In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of source code, privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, 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 [3].

8. Evaluated Configuration

The TOE is Sindoh MF2000, MF3000, MF4000, N610, N410 Series. The TOE is 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 Software Package. The TOE identification information is provided system report in LUI.

And the guidance documents listed in this report chapter 6, [Table 5] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] 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 EAL2.

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 clearly identifies the TOE and its all associated configuration items. Therefore the verdict PASS is assigned to ALC_CMC.2.

The configuration management document verifies that the configuration list includes the TOE, the parts that comprise the TOE, and the evaluation evidence. Therefore, the verdict of ALC_CMS.2 is the Pass.

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.

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 security architecture document is structured to ensure that TSF cannot be compromised or bypassed, and appropriately describes that the TSF which provides the security domain separates these domains from each other. Therefore, the verdict of ADV_ARC.1 is the Pass.

The functional specifications specifies the objective, way of using, input parameter, operation, and error message to the TSFI at equal detail level, and accurately and completely describes the TSFI. Therefore, the verdict of ADV_FSP.2 is the Pass.

The TOE design description provides the structure of the TOE in terms of subsystems, identify all subsystems of the TSF, and describe the behavior of each SFR-supporting or SFR-non-interfering. Therefore, the verdict of ADV_TDS.1 is the Pass.

Therefore, the security architecture document (the TSF architecture attribute which describes how to the TSF security enforcement is not compromised or bypassed), functional specification(TSF interface description) and design description, which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged 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.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 less than an enhanced-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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	PASS
	ALC_CMC.2	ALC_CMC.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
		ALC_DEL.1.2E	PASS	PASS	
	ALC_FLR.2	ALC_FLR.2.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.1	ADV_TDS.1.1E	PASS	PASS	PASS
		ADV_TDS.1.2E	PASS		
	ADV_FSP.2	ADV_FSP.2.1E	PASS	PASS	
		ADV_FSP.2.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
	ATE_COV.1	ATE_COV.1.1E	PASS	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 6] 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 TOE is assumed to be evaluated product under specific configuration settings in connection with TSF, administrator should operate the TOE according to the settings specified in Evaluated Configuration in evaluation technical report. Therefore, administrator should keep in mind that the TOE is not considered to be evaluated product if it is operated with different settings specified in the Evaluated Configuration.
- All of the external IT entities (User/Administrator's PC, External server, etc.) that communicate with the TOE over a network should support IPSEC protocol that is compatible with the security policy of the TOE. It should be remembered that all network communications are not allowed if there is no IPSEC channel to securely communicate with the TOE.
- For SNMPv1/v2 protocol provided by TOE, default policy is set to disable. When administrator uses SNMPv1/v2 protocol, administrator has to modify SNMPv1/v2 default community name.
- If IP filtering function is enabled, IP registered in IPSec policy must be registered in the IP filtering policy by the administrator so that users can access the TOE.
- If IP filtering function is enabled, IP registered in Administrator IP policy must be registered in the IP filtering policy by the administrator so that administrator can access the RUI.
- It should be noted that the TOE was evaluated in an environment where no wireless module was installed.
- Administrator only can manage for all of the security functions. Users who identified and authenticated by TOE can use the basic functions (print, scan, copy, fax) that allowed by the administrator.

11. Security Target

Sindoh MF2000, MF3000, MF4000, N610, N410 Series Security Target Version 1.3, March 27, 2017 [4] is included in this report by reference Security Target.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LUI	Local User Interface
RUI	Remote User Interface
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RFC	Request For Comments
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
PPM	Pages Per Minute
MMR	Modified Modified READ coding
MR	Modified READ Coding
MH	Modified Huffman Coding
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
U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy. Administrators may possess special privileges that provide capabilities to override portions of the TSP
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
U.USER	Any authorized User
Operation Panel	The MFP's panel that provides LUI for interacting with users to perform functions including security management and viewing the audit log
User data repository	The SD card or SSD (Solid-state disk) for storing user data

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 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] Sindoh MF2000, MF3000, MF4000, N610, N410 Series, Evaluation Technical Report V3.00, August 19, 2017

[4] Sindoh MF2000, MF3000, MF4000, N610, N410 Series, Security Target V1.3, March 27, 2017