KECS-CR-22-05

Sindoh MF2000, MF3000, MF4000, N620 Series Certification Report

Certification No.: KECS-CISS-1147-2022

2022. 1. 20.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2022.01.20	-	Certification report for Sindoh MF2000, MF3000, MF4000, N620 Series - First documentation

This document is the certification report for Sindoh MF2000, MF3000, MF4000, N620 Series of Sindoh Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory Co., Ltd. (KSEL)

Table of Contents

1. Executive Summary

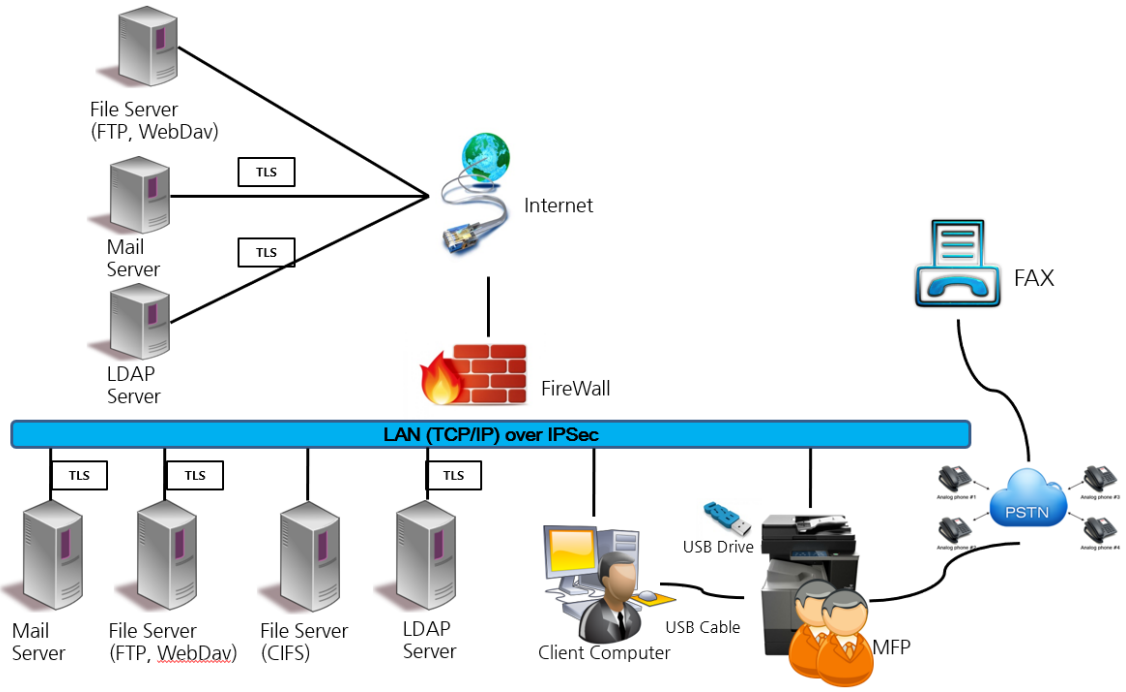
This report describes the certification result drawn by the certification body on the results of the EAL2 evaluation of Sindoh MF2000, MF3000, MF4000, N620 Series with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is multi-function peripherals (MFPs) which provides security features of identification and authentication, access control, security audit, security management, stored data protection, self-protection, fax data control, and trusted channel as well as copy, print, scan, and fax functions.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on 19 January 2022. This report grounds on the evaluation technical report (ETR) KSEL had submitted [5] and the security target (ST) [6][7].

The ST does not claim conformance to any protection profile. 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 both functional components in CC Part 2 and newly defined components in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE. The TOE is operated in an internal network protected by a firewall. External IT entities including client computers are connected to the TOE through IPSec connections. Users can connect to the TOE via LUI (local user interface, i.e., the operation panel) or RUI (remote user interface, i.e., web GUI). In order to access to web graphic user interface (GUI) provided by the TOE, the following software is necessary for the administrator’s PC: Chrome web browser version 92.0 or Microsoft Edge web browser version 92.0.



[Figure 1] Operational environment of 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 as follows.

TOE	Sindoh MF2000, MF3000, MF4000, N620 Series
Version	V211216_5
F/W Package	JUNIPER-R_Pkg_211216_5 - JUNIPER-R_Pkg_211126_5.zip
TOE Components (Firmwares)	JUNIPER-R_CTL :JUNIPER-R_211216_5 JUNIPER-R_EGB :05.07.57 JUNIPER-R_UICC :0.0.8 JUNIPER-R_DFC :02.23

	JUNIPER-R_BANK :1.02
Product Models	MF2085, MF3035, MF4061, MF4121, N620, N621, N622, N623
Guidance Document	Sindoh MF2000, MF3000, MF4000, N620 Series manual V1.3 (N620/MF Series) - Sindoh MF2000, MF3000, MF4000, N620 Series manual V1.3.pdf

[Table 1] TOE identification

The F/W package has five component firmwares, and those firmwares are installed in the boards of the TOE model during production. Note that all TOE models use the same firmware package. The guidance document is in PDF format on a CD-ROM. The product model is delivered to the customer in person together with the guidance document.

The following table shows the specifications of the TOE models.

MFP Product Model		**N620**	**N621**	**N622**	**N623**	**MF2085**	**MF3035**	**MF4061**	**MF4121**
Specification									
Copy speed (unit: ppm)		26	30	42	48	26	30	42	48
Memory(RAM)		2GB							
OP Type		10.1 inch Color TFT LCD							
CPU		1.2GHz Quad Core							
FAX module		Standard							
Storage	Default	eMMC: 8GB				eMMC: 8GB SD: 32GB			
	Expansion	SD (1 slot): 64GB SSD (1 slot): 256GB				SSD (1 slot): 256GB			
	MAX	eMMC: 8GB SD: 64GB SSD: 256GB				eMMC: 8GB SD: 32GB SSD: 256GB			

[Table 2] Hardware models and specifications

[Table 3] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Scheme for IT Security (May 17, 2021)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL2
Protection Profile	- (ST does not claim conformance to a PP)
Developer	Sindoh Co., Ltd.
Sponsor	Sindoh Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory Co., Ltd. (KSEL)
Completion Date of Evaluation	January 19, 2022
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [6][7] by security objectives and security requirements. Thus, the TOE provides the following security features:

- Identification and authentication: The TOE identifies and authenticates the users using ID and password. After predefined number of consecutive unsuccessful login attempts, the TOE locks an administrator account for predefined time duration and locks a normal user account until released by an administrator. An administrator can login to the TOE via both LUI and RUI, while the TOE provides the login interface via LUI for a normal user.
- Access control: The TOE controls access to the document data generated by print, scan, fax, and copy functions based on normal user ID. The TOE also

controls the execution of print, scan, fax, and copy functions based on normal user ID and role.

- Security Audit: The TOE generates audit records of security relevant events including fax log and audit log and stores them in the TOE.
- Security management: Security management of the TOE is restricted to only the authorized administrator who can access the management interface via LUI and RUI provided by TOE.
- Stored data protection: The TOE provides the function to encrypt the data on the user data repository (SD card or SSD). TOE also provides the function to overwrite the data from the user data repository.
- Self-protection: The TOE provides a set of self-test function that are executed when the TOE is started, periodically during normal execution, and at the request of the authorized administrator. The TOE also provides the authorized administrator with the capability to verify TSF and TSF data.
- Fax data control: The TOE restricts forwarding fax data received via PSTN to external interfaces unless explicitly allowed by an authorized administrative role.
- Trusted channel: The TOE provides trusted channels (IPSec, TLS) to protect user data or TSF data during communication with external IT entities including client computers through the network.

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][7], chapter 3.3):

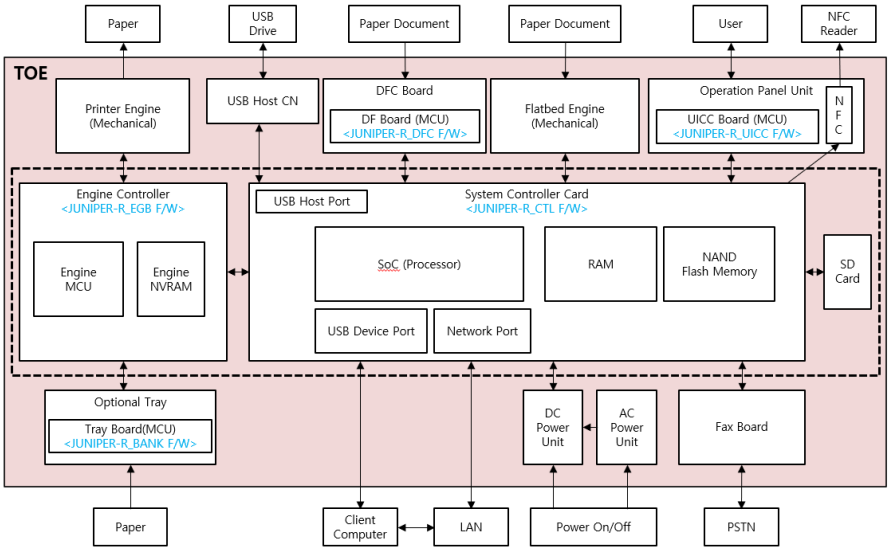
- The TOE must be in a physically safe environment, and protected from unauthorized physical accesses.
- TOE users must know the organizational security policies and procedures, and observe them.
- The administrator must observe the organizational security policies and procedures, be able to operate according to the TOE manufacturer's guideline and manual, complete operational education, and properly configure and operate the TOE according to the policies and procedures.
- Authorized TOE administrators should not be malicious, and should not abuse

their privileges.

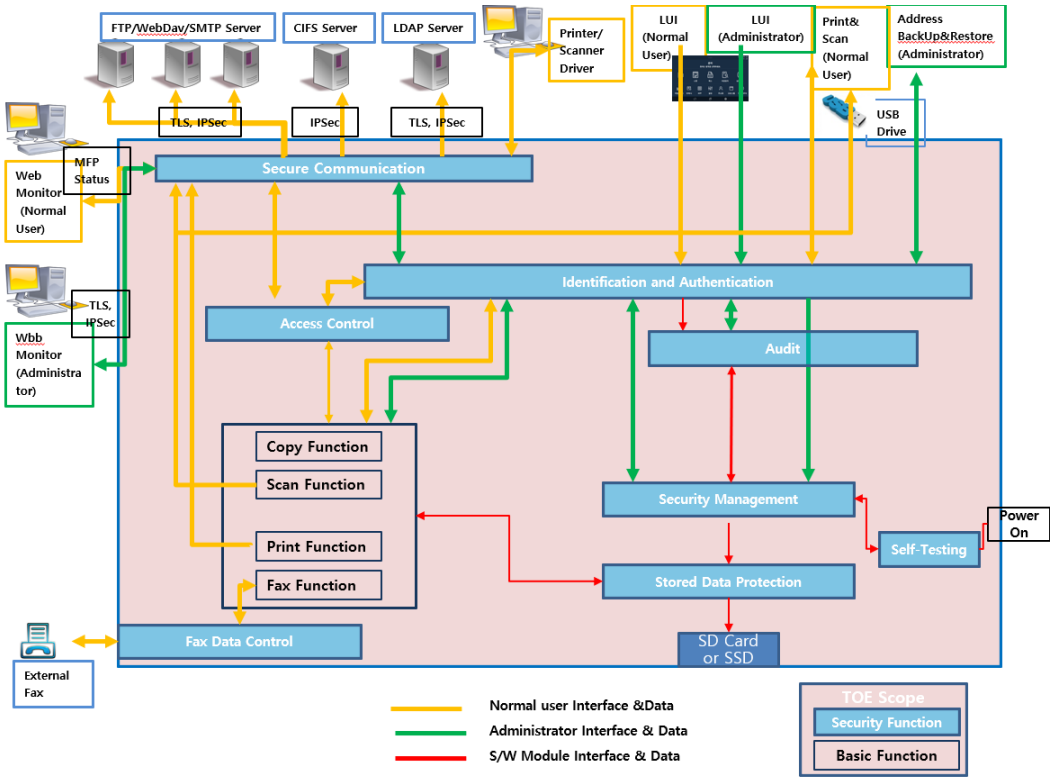
The assumptions defined in the ST, some aspects of threats, and organizational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment. Details can be found in the ST [6][7], chapter 3.1, 3.2 and 4.2.

5. Architectural Information

[Figure 2] and [Figure 3] show the architecture of the TOE. The TOE is MFPs that consists of five firmwares and eight product models (N620, N621, N622, N623, MF2085, MF3035, MF4061, MF4121). The firmwares are installed in the boards of the TOE model during production as shown in [Figure 2]. The TOE provides the security functions of identification and authentication, access control, security audit, security management, stored data protection, self-testing, fax data control, and secure communication as well as basic functions of copy, scan, print, scan, and fax as shown in [Figure 3].



[Figure 2] Physical structure of the TOE



[Figure 3] Logical scope of the TOE

6. Documentation

The following documentations are evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
Sindoh MF2000, MF3000, MF4000, N620 Series manual V1.3 (N620/MF Series)	V1.3	December 16, 2021

[Table 4] Documentation

7. TOE Testing

The developer took a testing approach based on the TSFIs provided by TOE based on

the 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. The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1. The evaluator prepared the TOE in accordance to the guidance document, performed all tests provided by developer, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is Sindoh MF2000, MF3000, MF4000, N620 Series (version V211216_5). See table 1 for detailed information on the TOE components.

The TOE is MFPs, and its component firmwares are installed in the boards of the TOE model during production. The guidance document is in PDF format on a CD-ROM. The product model is delivered to the customer in person together with the guidance document.

The TOE is identified by TOE name and version that includes build number. The TOE identification information is provided via Report.

The guidance documents listed in this report chapter 6, [Table 4] 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 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 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 Extended Components Definition has been clearly and unambiguously defined, and it is necessary. 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 describes how the TOE meets each SFR, 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 used 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 uses a CM system that uniquely identifies all configuration items. Therefore, the verdict PASS is assigned to ALC_CMC.2.

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.2.

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 configuration management 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 the 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. Therefore, the verdict PASS is assigned to ADV_TDS.1.
The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, for the SFR-enforcing TSFIs the developer has described the SFR-enforcing actions and direct error messages. Therefore, the verdict PASS is assigned to ADV_FSP.2.
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), 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 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 penetration 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, 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_CMC.2	ALC_CMC.2.1E	PASS	PASS	PASS
	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.1.1E	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_COV.1	ATE_COV.1.1E	PASS	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:

- All external IT entities including client computers and external servers that transmit/receive data to/from the TOE via the network must be configured to be compatible with the security policy of the TOE using the IPSec protocol. If the secure channel between the TOE and external IT entities was not implemented using IPSec protocol, it should be noted that all network communication with the TOE is blocked.
- It should be noted that all security management functions can only be performed by an authorized administrator. It should also be noted that only authorized normal users can use the basic functions (print, scan, copy, and fax) that was allowed by the administrator.
- The both SNMP version 1 and 2 provided by the TOE was set to disabled by default. If it is needed to use SNMP v1/v2 in the TOE, it should be noted that the default community name must be changed.
- The TOE continuously stores newly created audit data by overwriting the oldest audit data when the defined capacity (1000) of audit storage is exceeded. Therefore, it should be noted that old audit data may be overwritten by new audit data.
- When disposing of the TOE in use, be sure to delete the SD card/SSD so that important data is not exposed.
- 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 administrator IP must be registered initial installation procedure
- It should be noted that the TOE was evaluated in an environment where no wireless module was installed.

11. Security Target

Sindoh MF2000, MF3000, MF4000, N620 Series Security Target V1.9 [6] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [7] according to the CCRA supporting document ST sanitizing for publication [8].

12. Acronyms and Glossary

CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
GUI	Graphic User Interface
IPSec	Internet Protocol Security
LUI	Local User Interface
MFP	Multi-Function Peripheral
PSTN	Public Switched Telephone Network
RUI	Remote User Interface
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSD	Solid State Drive
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

Local User Interface (LUI)	Interface for U.NORMAL and U.ADMINISTRATOR to access, use, or manage the MFP directly in the operation panel
Multi-Function Peripheral (MFP)	MFP is a machine that incorporates the functionality of multiple devices (copy, print, scan, or fax) in one
Remote User Interface (RUI)	Interface for U.NORMAL and U.ADMINISTRATOR to

	access, use, or manage the TOE via web service
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.
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE

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 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
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 5, CCMB-2017-04-004, April 2017

[3] Korea Evaluation and Certification Guidelines for IT Security (24 August 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (17 May 2021)

[5] KSEL-CC-2021-07 Sindoh MF2000, MF3000, MF4000, N620 Series Evaluation Technical Report V3.00, 19 January 2022

[6] Sindoh MF2000, MF3000, MF4000, N620 Series Security Target V1.9, 12 January 2022 (Confidential Version)

[7] Sindoh MF2000, MF3000, MF4000, N620 Series Security Target (ST Lite) V1.1, 12 January 2022 (Sanitized Version)

[8] ST sanitizing for publication, CCDB-2006-04-004, April 2006