KECS-CR-20-49

Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series

Certification Report

Certification No.: KECS-CISS-1035-2020

2020. 8. 26

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2020.8.25	-	Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series - First documentation

This document is the certification report for Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series from HP Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory (KSEL)

Table of Contents

1. Executive Summary

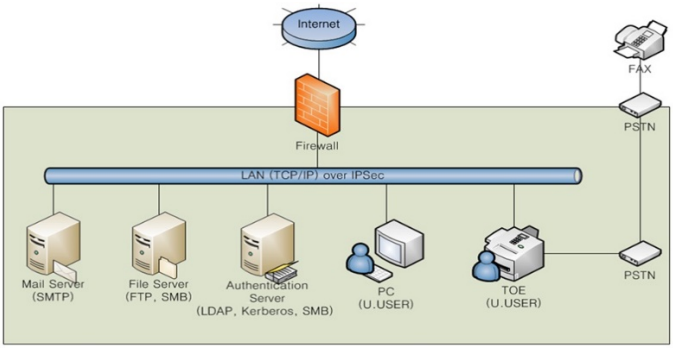
This report describes the results of the EAL2+ evaluation of Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series from HP Inc. with reference to the Common Criteria for Information Technology 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 August 14, 2020. This report grounds on the evaluation technical report (ETR) [3] KSEL had submitted and the Security Target (ST) [4]. The ST has conformance claim to U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std.2600.2™-2009) [5].

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 augmented by ALC_FLR.2. 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 identifies the extended security functional requirement. The extended SFR component (FPT_FDI_EXP Restricted forwarding of data to external interfaces) has been clearly and unambiguously defined. 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.USER 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.USER can also use their PCs to print out documents or to access the TOE through the internal network. U.ADMINISTRATOR can enable/disable Automatic Image Overwrite, start/stop Manual Image Overwrite, 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, and download the security audit report. The U.USER's account information that requires asking for internal authentication by the TOE can be stored on the hard disk drive of the TOE. All of the information stored on the hard disk drive is protected by the TOE. In the case of external authentication using Kerberos, LDAP, SMB server, the external authentication servers will perform the user authentication using database of authentication server. The 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 identified as follows:

TOE Name	Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series
TOE Version	H6.02
System Firmware	V5.H6.02(Samsung_K4350_Series_V5.H6.02.hds) V6.H6.02(Samsung_X4300_Series_V6.H6.02.hds) V5.H6.02(Samsung_K7600_Series_V5.H6.02_ALL.hds) V6.H6.02(Samsung_X7600_Series_V6.H6.02_ALL.hds)
MFP Product Model	K4250RX, K4300LX, K4350LX, K401LX, X4220RX, X4250LX, X4300LX, X401LX, X400LX, K7400LX, K7500LX, K7600LX, K7600GX, X7400LX, X7500LX, X7600LX, X7600GX, X704LX, X706GX, K705LX, K706GX

[Table 1] TOE identification

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (September 12, 2017)
TOE	Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series
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+ (EAL2 augmented by ALC_FLR.2)
Protection Profile	U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std.2600.2™-2009)
Developer	HP Printing Korea Co., Ltd
Sponsor	HP Inc.
Evaluation Facility	Korea Security Evaluation Laboratory Co., Ltd.
Completion Date of Evaluation	August 14, 2020
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

[Table 3,4,5] shows the general specification for the TOE.

MFP Product Model		X4220RX	X4250LX	X4300LX	X400LX	X401LX	K4250RX	K4300LX	K4350LX	K401LX
Color /Mono		Color	Color	Color	Color	Color	Mono	Mono	Mono	Mono
PPM		22ppm	25ppm	30ppm	24ppm	29ppm	25ppm	30ppm	35ppm	34ppm
Processor		Chorus4N (Dual Core : Cortex-A9 1000MHz, ARM9 250MHz)								
RAM		DDR3 2,048MB					DDR3 2,048MB			
ROM		NAND 128MB					NAND 128MB			
Interface		High-Speed USB 2.0 Host, High-Speed USB 2.0 Peripheral, Ethernet 10/100/1000 Base TX								
FAX		Option Kit, ITU-T G3, Super G3, 33.6 Kbps, MH/MR/MMR/JBIG								
HDD		SATA2 320 GB								
Display (LUI)	General Spec	10.1” 1024 x 600 WSVGA TFT Color Graphic LCD with Touch-Screen, 24-bit color								
	Processor	Quad Core (Cortex-A7, 1GHz)								
	RAM	2GB RAM								
	ROM	4GB ROM								

[Table 3] General Specification for the TOE

MFP Product Model		X7400LX	X7500LX	X7600LX	X7600GX	K7400LX	K7500LX	K7600LX	K7600GX
Color /Mono		Color	Color	Color	Color	Mono	Mono	Mono	Mono
PPM		40ppm	50ppm	60ppm	60ppm	40ppm	50ppm	60ppm	60ppm
Processor		A3000 (1.5GHz)							
RAM		DDR3 4,096MB							
ROM		NAND 4,096MB							
Interface		High-Speed USB 3.0 Host, High-Speed USB 3.0 Peripheral, Ethernet 10/100/1000 Base TX							
FAX		ITU-T G3, Super G3, 33.6 Kbps, MH/MR/MMR/JBIG							
HDD		SATA2 320 GB							
Scanner		DSDF (Dual Scan Document Feeder) 80 IPM (LX model)/120 IPM (GX model)							
Display (LUI)	General Spec	10.1” 1024 x 600 WSVGA TFT Color Graphic LCD with Touch-Screen, 24-bit color							
	Processor	Quad Core (Cortex-A7, 1GHz)							
	RAM	2GB RAM							
	ROM	4GB ROM							

[Table 4] General Specification for the TOE

MFP Product Model		X704LX	X706GX	K705LX	K706GX
Color /Mono		Color	Color	Mono	Mono
PPM		39ppm	59ppm	49ppm	59ppm
Processor		A3000 (1.5GHz)			
RAM		DDR3 6GB			
ROM		eMMC 4GB			
Interface		High-Speed USB 3.0 Host, High-Speed USB 3.0 Peripheral			
		Ethernet 10/100/1000 Base TX			
FAX		ITU-T G3, Super G3, 33.6 Kbps, MH/MR/MMR/JBIG			
HDD		SATA2 320 GB			
Scanner		DSDF			
		Up to A3 size			
Display (LUI)	General Spec	10.1” 1024 x 600 WSVGA TFT Color Graphic LCD with Touch-Screen, 24-bit color			

[Table 5] General Specification for the 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

4.1 Assumptions

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 (A.ACCESS.MANAGED).
- 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.USER.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 to correctly configure and operate the TOE in accordance with those policies and procedures (A.ADMIN.TRAINING).
- Administrators do not use their privileged access rights for malicious purposes (A.ADMIN.TRUST).

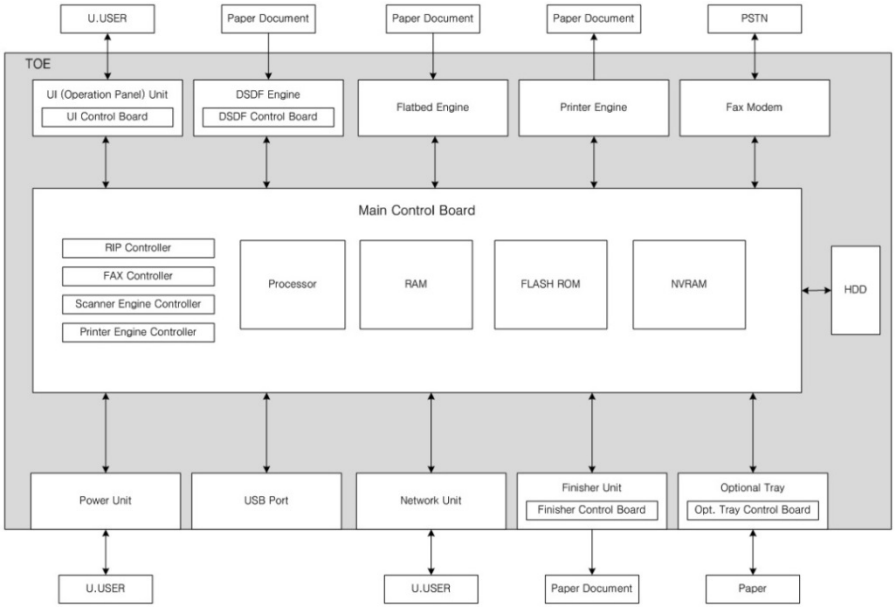
4.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the MFP needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

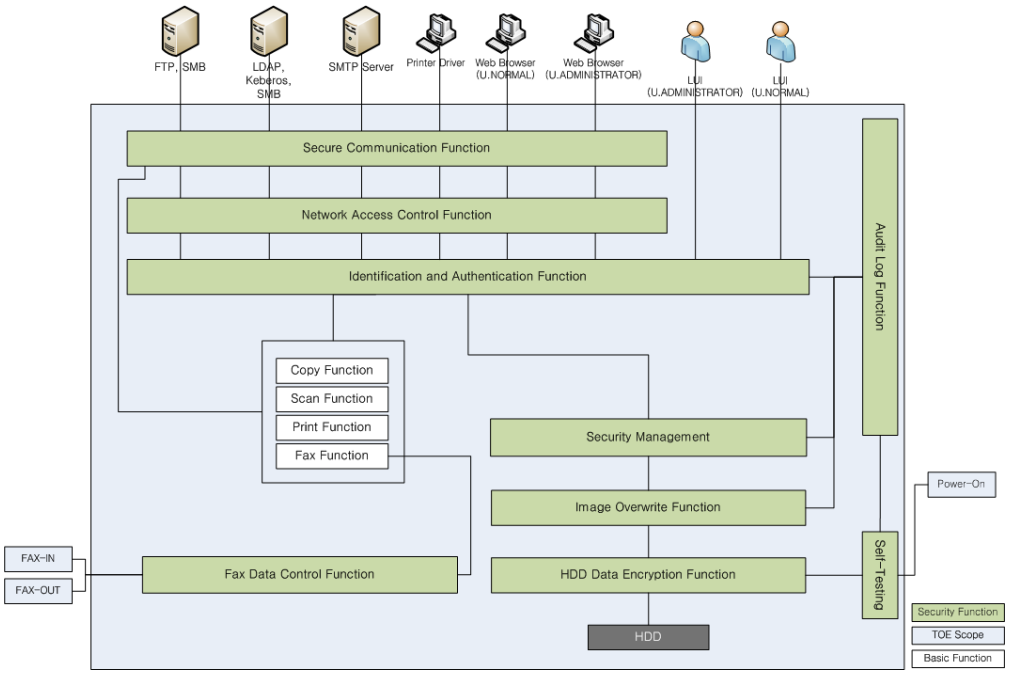
Note that: this evaluation covers only the specific TOE Version and MFP Product Models as identified in this document, and not any earlier or later versions released or in process.(for the detailed information of TOE Version and MFP Product Models refer to the [Table 1], [Table 3,4,5])

5. Architectural Information

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



[Figure 2] Physical Structure of MFP



[Figure 3] Logical scope of the TOE

The following security functions are provided by the TOE:

- **Identification & Authentication**

The TOE provides two types of user identification and authentication methods. If U.ADMINISTRATOR configures the local authentication, the MFP will authenticate the U.USER against an internal database. If U.ADMINISTRATOR selects the external authentication as an authentication method, then MFP will authenticate the U.USER using an external authentication server.

U.USER should be identified and authenticated by entering both ID and Password to access to the TOE management functions. If U.USER fails to login specific times, the system blocks the session of the U.USER during predefined duration.

U. ADMINISTRATOR can configure Identification & Authentication Policy by using LUI or RUI.

U. ADMINISTRATOR can also give specific permission for U.USER to only use certain feature of the machine.

The TOE provides the Common Access Control & TOE Function Access Control based on the user role assigned to a user group ID by U.ADMINISTRATOR when U.NORMAL performs read/delete/modify operations on the data owned by U.NORMAL or when U.NORMAL accesses print/scan/copy/fax functions offered by the MFP.

The TOE shall terminate an interactive session after predefined time interval of user inactivity.

- **Network Access Control**

The MFP system has a network interface connected to a network. The MFP system can send/receive data and MFP configuration information and thus is able to configure MFP settings.

There are a couple of methods to access and communicate with the MFP from outside of the TOE through the network, and the TOE manages all incoming packets via a network interface.

1) Protocol and Port Control:

The TOE can only allow protocols and ports configured by U.ADMINISTRATOR.

U.ADMINISTRATOR can configure this information via the LUI or RUI.

2) IP and MAC address filtering:

U.ADMINISTRATOR can make filtering rules for IP addresses and MAC addresses.

After that, packets are only allowed as per the IP filtering rule registered by U.ADMINISTRATOR. Packets via MAC addresses registered by U.ADMINISTRATOR

are not allowed.

- **Security Management**

The TOE accomplishes security management for the security function, TSF data, and security attribute.

Only U.ADMINISTRATOR can manage the security functions through the LUI (Local User Interface) and RUI (Remote User Interface): security functions can be start and stop by U.ADMINISTRATOR. The LUI is touch-screen based management service which is provided by TOE. RUI is web-based management service using HTTP/HTTPS protocol.

TSF data and their possible operations are specified by U.ADMINISTRATOR.

Security attributes can be operated by U.ADMINISTRATOR.

- **Security Audit Data**

The TOE creates an audit record security audit event including job log, security event log, and operation log. The audit data consist of the type of event, date and time of the event, success or failure, log out and access of log data.

Only U.ADMINISTRATOR is authorized to view (or export) the audit data but even U.ADMINISTRATOR shall not delete log data manually.

The TOE protects Security Audit Data stored on the hard disk drive. It prevents any unauthorized alteration to the Security Audit Data, and when each log events exceeds the maximum number, the TOE overwrites the oldest stored audit records and generates an audit record of overwriting.

- **Image Overwrite**

The TOE provides Image Overwrite functions that delete the stored file from the MFP's hard disk drive. The Image Overwrite function consists of Automatic Image Overwrite and Manual Image Overwrite. The TOE implements an Automatic Image Overwrite to overwrite temporary files created during the copying, printing, faxing and scanning (scan to e-mail, scan to FTP, and scan to SMB task processes). The image overwrite security function can also be invoked manually only by U.ADMINISTRATOR through the LUI. Once invoked, the Manual Image Overwrite cancels all print and scan jobs, halts the printer interface (network), overwrites the hard disk according to the procedures set by U. ADMINISTRATOR. If there are any problems during overwriting, the Manual Image Overwrite job automatically restarts to overwrite the remaining area.

- **Data Encryption**

The TOE provides an encryption function during the data storage procedure and a decryption function in the process of accessing stored data from hard disk drive.

The TOE generates cryptographic keys when the TOE is initialized at the first setout the secret key (256 bits) is used for encrypting and decrypting user data and TSF data that is stored on the HDD. Access to this key is not allowed to any U.USER including U.ADMINISTRATOR.

The TSF shall destroy cryptographic keys in accordance with overwriting a used cryptographic key with a newly generated cryptographic key. Before storing temporary data, document data, and system data on the HDD of the MFP, the TOE encrypts the data using AES 256 algorithm and cryptographic key.

When accessing stored data, the TOE decrypts the data using the same algorithm and key. Therefore, the TOE protects data from unauthorized reading and falsification even if the HDD is stolen.

- **Fax Data Control**

If the received fax data includes malicious content, it may threaten the TOE asset. To prevent this kind of threat, the TOE inspects whether the received fax image is standardized with MMR, MR, or MH of T.4 specification or not before forwarding the received fax image to e-mail or SMB/FTP. U. ADMINISTRATOR can restrict this forwarding function. When non-standardized format data are discovered, the TOE destroys the fax image.

- **Self Testing**

During initial start-up, the TOE performs self test. Self testing executes TSF function to verify the correct operation of the HDD encryption function. Also, the TOE verifies the integrity of the encryption key data and TSF executable code by the self testing.

- **Secure Communication**

The TOE also provides secure communication between the TOE and the other trusted IT product to protect communicated data from modification or disclosure by IPSec. The network which connected without IPSec shall not be allowed to communicate with MFP.

6. Documentation

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

Identifier	Version
Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series User's Guide	V0.2
Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series Installation Guide	V0.2

[Table 6] 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 the 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 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 Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series. This 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 TOE is identified by TOE name and version number including release number. The TOE identification information is provided via GUI and Report.

And the guidance documents listed in this report chapter 6, [Table 6] 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 (ST reference, TOE reference, TOE overview and TOE description), and these four 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 clearly and unambiguously defines the extended SFR component

(FPT_FDI_EXP.1). 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 configuration management document describes the method used to uniquely identify all configuration items. Therefore, the verdict PASS is assigned to ALC_CMC.2.

The configuration list includes the TOE itself, the evaluation evidence required by the SARs, and the parts that comprise the TOE. Therefore, the verdict PASS is assigned to ALC_CMS.2.

The delivery documentation describes all procedures that are necessary to maintain security when distributing the TOE to the user. Therefore, the verdict PASS is assigned to ALC_DEL.1.

The flaw remediation procedures are established and they provide for the correctness of security flaws and for assurance that the corrections introduce no new security flaws. Therefore, the verdict PASS is assigned to ALC_FLR.2.

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 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 PASS is assigned to ADV_ARC.1.

The functional specifications specifies the purpose of an interface, method of use, input and output parameters, actions of an interface, and error messages generated by the TSF at equal detail level, and accurately and completely describes the TSFI. Therefore, the verdict PASS is assigned to ADV_FSP.2.

The TOE design description provides the structure of the TOE in terms of subsystems, identifies all subsystems of the TSF, describes the behavior summary of each SFR-supporting or SFR-non-interfering TSF subsystems, and summarizes the SFR-enforcing behavior of the SFR-enforcing subsystems. Therefore, the verdict PASS is assigned to ADV_TDS.1.

Therefore, the security architecture description(the TSF architecture attribute which describes how to the TSF security enforcement is not compromised or bypassed), functional specification(TSF interfaces description) and TOE 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 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	
		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_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_IND.2.3E	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 7] 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:

- There are possibilities that the data stored on the TOE are exposed to an attacker in an unauthorized manner if the TOE is carried out of an organization without deleting the stored file from the MFP's hard disk drive. Therefore, make sure of using Manual Image Overwrite function to overwrite the critical and sensitive data when the TOE is taken out of an organization for repair, replacement, disuse, etc.
- All of the external IT entities (User/Administrator's PC, External storage server, External authentication server, NTP 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.
- If there are any problems, such as blackout or power failure, during manual image overwriting, the image overwriting function is terminated remaining the image overwriting of the memory area uncompleted. Therefore, administrator should keep in mind that the manual image overwriting function automatically restarts to overwrite the remaining memory area if the power is supplied again.
- Use the TOE function "Login IPv4 Address Protect" to register the allowed administrator's IP so that unauthorized access can be blocked.

11. Security Target

Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series Security Target V0.3[4] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LDAP	Lightweight Directory Access Protocol
MH	Modified Huffman Coding
MMR	Modified Modified READ(Relative Element Address Designate) coding
MR	Modified READ(Relative Element Address Designate) coding
OR	Observation Report
PP	Protection Profile
PPM	Pages Per Minute
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
Image Overwrite	This is a function to delete all stored files on the hard disk drive. There are two kinds of image overwriting: Automatic Image Overwrite and Manual Image Overwrite
Automatic Image Overwrite	The Automatic Image Overwrite automatically carries out overwriting operations on temporary image files at the end of each job such as copy, scan, scan-to-email, scan-to-FTP, or scan-to-SMB. Or the Automatic Image Overwrite overwrites the files on the hard disk drive when a user initiates a delete operation
Manual Image Overwrite	The Manual Image Overwrite function overwrites all

	stored files, including image files and preserved files on the hard disk drive, and the function should only be manually performed by a U.ADMINISTRATOR through the LUI. The image data is completely overwritten by using DoD 5220.28-M, DoD 5220.28-M(ECE), Australian ACSI 33, VSITR(German standard) standard, and Custom setting methods
Image file	Temporarily stored file that is created during scan, copy, or fax job processing
LUI, Local User Interface	Interface for U.NORMAL or U.ADMINISTRATOR to access, use, or manage the MFP directly
RUI, Remote User Interface	Interface for U.NORMAL or U.ADMINISTRATOR to access, use, or manage the TOE through a web service
MFP, Multi-Function Printer	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.
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
U.USER	Any authorized User. There may be two types of Users: U.NORMAL and U.ADMINISTRATOR.

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

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3] Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series, Evaluation Technical Report V1.00, August 14, 2020

[4] Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series Security Target V0.3, August 3, 2020

[5] U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std.2600.2™-2009)