Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan
2-28-8, Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2017-12-11 (ITC-7657)
Certification Identification	JISEC-C0598
Product Name	MX-B455W / B355W with MX-FR59U
Version and Release Numbers	0210mc00
Product Manufacturer	SHARP CORPORATION
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)
Assurance Package (optional)	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1
Name of IT Security Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE has been certified as follows.
2018-05-22

Fumiaki Manabe, Technical Manager
Information Security Certification Office
IT Security Center, Technology Headquarters

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass

"MX-B455W / B355W with MX-FR59U 0210mc00" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the

specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1 Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "MX-B455W / B355W with MX-FR59U version 0210mc00" (hereinafter referred to as the "TOE") developed by SHARP CORPORATION, and the evaluation of the TOE was finished on 2018-04 by Information Technology Security Center Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, SHARP CORPORATION, and provide security information to procurement entities and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "general consumers who purchase this TOE" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is the following assurance components of CC Part 3.

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

1.1.2 TOE and Security Functionality

This TOE is an IT product and a digital multifunction device (hereinafter referred to as the "MFD") equipped not only with copy, printer, scanner and fax function, but also with a function to save and retrieve documents (referred to as the "document filing function" in this TOE).

This TOE provides security functions required by the Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 [14][15] (referred to as the "Conformance PP")

which is the Protection Profile for the MFD, to prevent unauthorized exposure and tampering of the data handled by the MFD.

For these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated based on the CEM as well as the assurance activities of the Conformance PP within the scope of the assurance package.

The threats and assumptions that the TOE assumes are described in the next section.

1.1.2.1 Threats

This TOE assumes the following threats.

There is a threat of unauthorized exposure or tampering of the user document data and the data affecting the security functions which are the protected assets of the TOE in the operation of the TOE or access to the network to which the TOE is connected.

There is also a threat of damaging the security functions of the TOE due to the failure of the TOE itself or installation of unauthorized software.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

It is assumed that the TOE is operated in an environment where unauthorized physical access is restricted and it is connected to a LAN protected from the Internet.

The management and maintenance of the TOE under operation must be appropriately performed by an administrator trusted by the procurement entities in accordance with the guidance documents. In addition, users of the TOE must be trained to use the TOE securely.

1.1.3 Disclaimers

In this evaluation, the operations shown below are out of the scope of assurance.

- Operation in a state where the operational environment of the TOE shown in "4.3 Clarification of Scope" is not secure
- Operation of the TOE under conditions other than those indicated in "7.5 Evaluated Configuration"

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2018-04, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure.

The Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]).

The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2 Identification

The TOE is identified as follows:

TOE Name: MX-B455W / B355W with MX-FR59U
TOE Version: 0210mc00
Developer: SHARP CORPORATION

The TOE name consists of the MFD main unit and mandatory option. TOE components are shown in Table 2-1.

Table 2-1 TOE Components

Main unit		Mandatory option
Model number	Sales territory	
MX-B455W	Japan / Other than Japan	MX-FR59U
MX-B355W	Other than Japan	MX-FR59U

Users can verify that a product is the evaluated and certified TOE by the following means.

The following information indicated on the casing of the TOE and the operation panel should be confirmed in accordance with the description in the product guidance.

・Model number of main unit:

The model number of main unit indicated on the casing shall be the name contained in "Model number" of Table 2-1.

・Mandatory option:

The option name indicated on the operation panel shall match the name contained in "Mandatory option" corresponding to "Model number" in Table 2-1.

・TOE version:

The TOE version indicated on the operation panel shall match the TOE identification version.

3 Security Policy

The TOE provides MFD basic functions such as copy function, printer function, scanner function, fax function and document filing function. It has the functions to store user's document data inside the TOE as well as to communicate with user's terminals and various servers via the network.

The TOE provides the following security functions that satisfy the requirements of the Conformance PP.

- A function to identify and authenticate users
- A function to control access to user data
- A function to encrypt and store user data
- A function to protect user data on the communication paths when using the LAN
- A function to restrict security management to the identified and authenticated users
- A function to log events related to security
- A function to verify and install updated firmware
- A function to verify normal operation of security functions at start-up
- A function to separate the PSTN and LAN
- A function to overwrite data under processing such as copy function at the completion or cancellation
- A function to delete all user data completely

Details of the basic functions and security functions of the TOE are shown in Section 5.1.

Details of the user roles, protected assets, threats and organizational security policies assumed by the TOE are shown in Sections 3.1 to 3.4.

3.1 User Roles

Users shown in Table 3-1 are assumed in the use of the TOE.

Table 3-1 User Roles

Name	Type	Definition
U.NORMAL	Normal User	A User who has been identified and authenticated and does not have an administrative role
U.FAX	Fax User	A Normal User who has been identified and authenticated and granted access authority to fax reception data
U.ADMIN	Administrator	A User who has been identified and authenticated and has an administrative role

3.2 Protected Assets

The protected assets of the TOE can be classified into two types as shown in Table 3-2 below. Among the two types of protected assets, the user data is shown in Table 3-3, and TSF data is shown in Table 3-4. Each of these two types of protected assets is composed of further two types of protected assets.

Table 3-2 Protected Assets of the TOE

Name	Type	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

Table 3-3 Protected Assets (User Data)

Name	Type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

Table 3-4 Protected Assets (TSF Data)

Name	Type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3 Threats

The TOE assumes threats described in Table 3-5.

Table 3-5 Assumed Threats

Name	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.

Name	Definition
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 Organizational Security Policies

Organizational security policies required for use of the TOE are described in Table 3-6.

Table 3-6 Organizational Security Policies

Name	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
P.PURGE_DATA	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.

4 Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE.

The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Name	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2 Environmental Assumptions

The TOE is installed in an office and connected with the PSTN and LAN which is the internal network of the organization, and used with a client PC and various servers similarly connected to the LAN.

Figure 4-1 shows the general operational environment as assumptions of the TOE.

Users use the TOE by operating the operation panel of the TOE or a PC connected to the LAN.

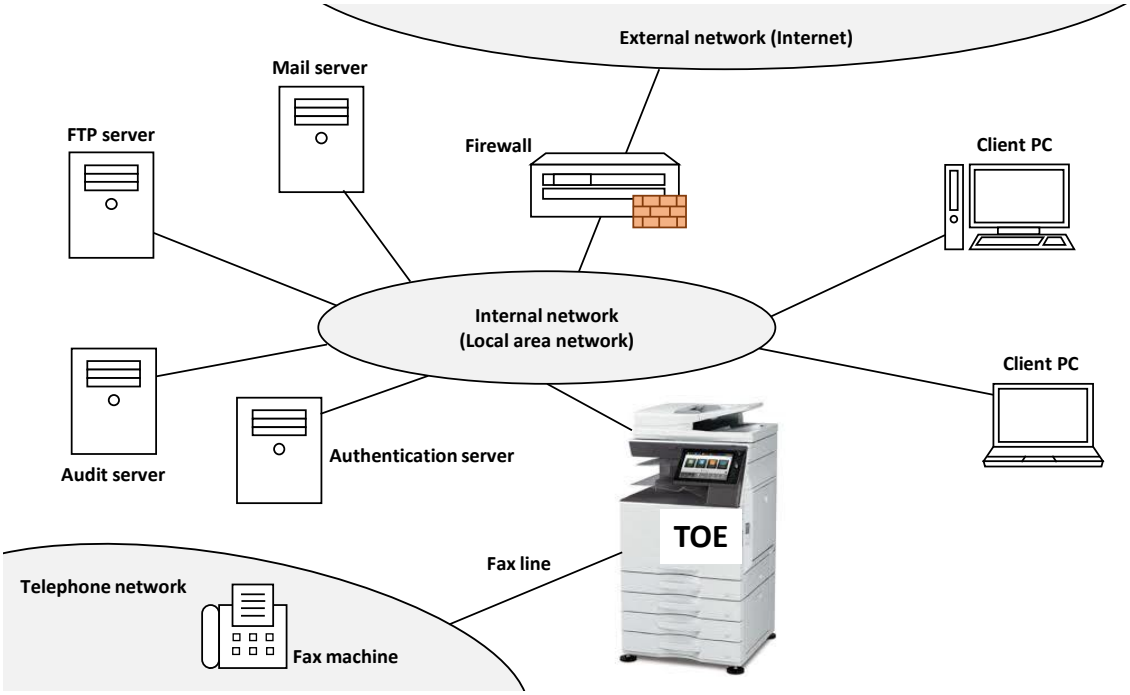

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

(1) Client PC

It is a general PC used by users.
The following software are required for use of the TOE.

- Printer Driver

  The name for the TOE of which sales territory is other than Japan is "SHARP <model number of main unit> PCL6 Driver", and the name for the TOE of which sales territory is Japan is "SHARP <model number of main unit> SPDL2 Driver." The "<model number of main unit>" means either one of the model number of main unit in Table 2-1.

- Web Browser

(2) Audit Server

It is an audit server to store the audit log generated by the TOE. It must use the syslog protocol and support TLS v1.2. Installation of this server is mandatory.

(3) Authentication Server

In the case of "external authentication method" shown in "Identification and authentication function" in Section 5.1.2, an authentication server which supports

TLS v1.2 and of which authentication protocol is LDAP authentication method is required.

(4) Mail Server

It is necessary to send user document data scanned using the "Scanner function" as an E-mail attached file. It must support TLS v1.2.

(5) FTP Server

It is necessary to send user document data scanned using the "Scanner function" to the specified FTP server. It must support TLS v1.2.

It should be noted that the reliability of the hardware and the cooperating software shown in this configuration is out of the scope in the evaluation. It is assumed to be trustworthy.

4.3 Clarification of Scope

In the TOE, a server such as an authentication server may be installed in addition to the audit server that is mandatory to install. In addition, it is necessary to install a firewall to connect to the Internet which is an external network. It is the responsibility for the operators that these servers and firewalls are operated securely according to security objectives.

5 Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE.

The area enclosed by the frame indicated as the "TOE" in Figure 5-1 is the TOE. It does not include Audit server, Mail server, FTP server, Authentication server, Client PC, User and External fax machine.

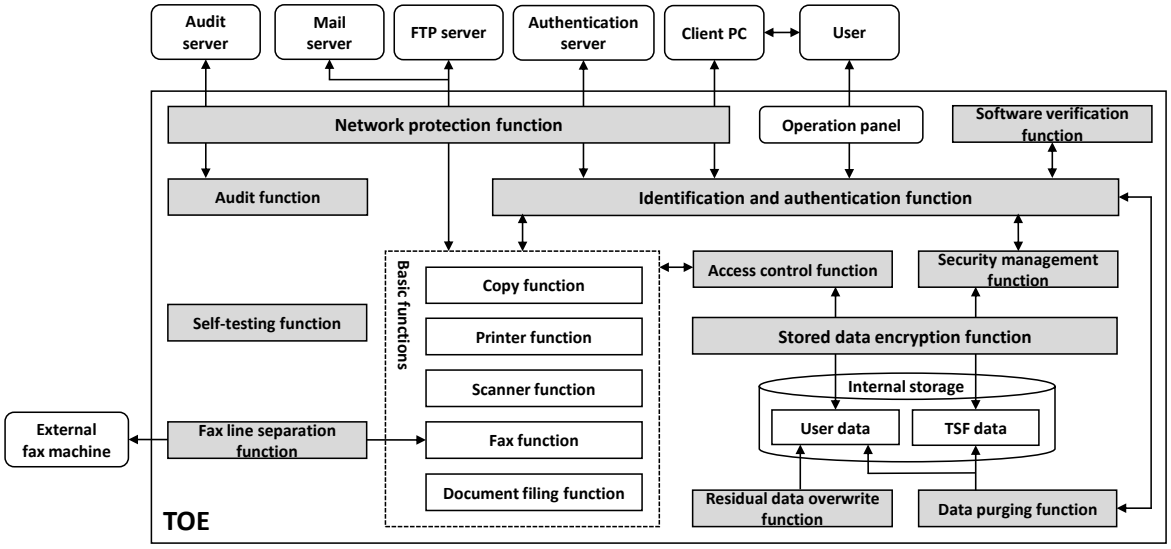

Figure 5-1 TOE boundary

The basic functions (functions shown in white box) of the TOE and the security functions (functions shown in shaded box) in Figure 5-1 are described below.

5.1.1 Basic Functions

(1) Copy function

It is a function to copy and print the user document data scanned from paper documents by user's operation from the operation panel.

(2) Printer function

It is a function to receive the user document data via the LAN from the printer driver of the client PC and print it by user's operation from the operation panel.

(3) Scanner function

It is a function to scan paper documents and send the scanned user document data to the mail server and FTP server by user's operation from the operation panel.

(4) Fax function

It is a function to send and receive the document data to and from external fax machines conforming to the G3 standard connected by the PSTN. It consists of the fax transmission function, in which paper documents are scanned and the scanned document data are sent to the external fax machine, and the fax reception function, in which document data sent from an external fax machine are received and printed by user's operation.

(5) Document filing function

It is a function to store the user document data in the internal storage of the TOE at the same time with the copy function, etc., and to print the stored user document data by user's operation from the operation panel or from the client PC via the LAN.

5.1.2 Security Functions

(1) Identification and authentication function

It is a function to identify and authenticate users of the TOE by login names and passwords in the operation panel, the web browser of the client PC, and the printer driver.

- It requests a password consisting of upper or lower case letters of the alphabet, numbers, or special characters and having the number of characters set by the administrator or more.
- It supports "internal authentication method" using user information stored in the TOE and "external authentication method" using external authentication server.
- When entering a password, it displays an asterisk instead of the input character.
- It stops accepting authentication for 5 minutes if password authentication has failed consecutively.
- After identification and authentication, the session is terminated if no operation is performed for the time set by the administrator in the case of the operation panel, or for 5 minutes in the case of the web browser.

(2) Access control function

It is a function to control access of user data when manipulating user data with the basic functions of the TOE.

- It controls access to user data based on the policy defined for each type of user such as owner of user data or user role.

(3) Stored data encryption function

It is a function to encrypt and store user data, etc., in the TOE.

- User data and TSF data are encrypted by AES CBC mode with a 256-bit key and stored.
- An encryption key for encrypting user data, etc., is created by a random number generator having sufficient entropy.

(4) Network protection function

It is a function to protect user data on the communication path when using the LAN.

- Encrypted communication by TLS v1.2 is used between the TOE and various servers such as audit server.
- The encryption key used for encrypted communication is created by a random number generator having sufficient entropy and is stored only in the volatile memory.
- In the communication between the client PC and the TOE, IPP over TLS communication is used for the printer driver, and HTTPS communication is used for the web browser.

(5) Security management function

It is a function to restrict the security management of the TOE to the identified and authenticated users.

- Registration / deletion of internal authentication users, change of minimum password length, setting of various servers, overwriting of user data and TSF data, etc., are provided only to users with the administrator role.
- Inquiries about user login names and user roles of the users themselves, and change of passwords are provided to all internal authentication users.

(6) Audit function

It is a function to log events related to use of the TOE and security.

- In addition to the start and end of the audit, a log of the audit event such as the end of the job and failure of identification and authentication is generated as audit data. In the audit data, the event name, date and time of occurrence, user login name, event result and additional information are recorded.
- The generated audit data is sent to the audit server by using the syslog protocol and TLS v1.2.

(7) Software verification function

It is a function that the TOE verifies the update firmware and enables installation of only legitimate firmware.

- It verifies that it is a legitimate firmware by checking the hash value of the firmware with a digital signature provided at the same time as the firmware and the hash value calculated by the TOE using SHA - 256.
- A user with the administrator role can acquire the version of the firmware.

(8) Self-testing function

It is a function to verify the normal operation of the security functions at the start-up of the TOE.

- Verification that the security functions operate normally is done by the entropy source health test of the random number generator, by the known answer test of the encryption algorithm, and by confirming that the firmware is not corrupted.
- In the verification, if any error is detected in all or in part, the TOE stops the start-up and suspends any operation until the power is turned off.

(9) Fax line separation function

It is a function to separate the public switched telephone network (PSTN) and LAN.

- In order to protect the LAN against attacks from the PSTN, it restricts inputs from the PSTN to fax reception and prohibits forwarding of the received fax.

(10) Residual data overwrite function

It is a function to overwrite data under processing such as copy function at the completion or cancellation.

- It overwrites the user document data with the value set by the administrator at the end of the document job.

(11) Data purging function

It is a function to completely delete user data, etc.

- It overwrites all user data and TSF data on the internal storage according to the request of the user with the administrator role. At this time, the encryption key for stored data encryption is regenerated.

5.2 IT Environment

The TOE communicates with various servers and client PCs via the LAN.

The TOE sends the generated audit data to the audit server. The administrator reads the audit data from the audit server.

In the case of the external authentication method, the authentication server is used to identify and authenticate users.

The TOE can send the scanned user document data to the mail server and FTP server.

6 Documentation

The identification of documents attached to the TOE is shown in Table 6-1.

TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Attached Documents

Name	Version	Language
スタートガイド	TINSJ2333QSZZ HH1	Japanese
かんたん操作ガイド	2017L-JP1	Japanese
ユーザーズマニュアル	2017L-JP1	Japanese
Web ページ設定ガイド	2017H-JP1	Japanese
ソフトウェアセットアップガイド	2017L-JP1	Japanese
Q&A 集 (困ったときのガイド)	2017L-JP1	Japanese
取扱説明書 データセキュリティキット MX-FR59U	JP1	Japanese
注意書 データセキュリティキット MX-FR59U	1.0	Japanese
Protection Profile for Hardcopy Devices 適合状態で MX-FR59U をご利用のお客様へ	V1.0	Japanese
Start Guide	TINSX2335QSZZ HH1	English
Quick Start Guide	2017L-EX1	English
User's Manual	2017L-EX1	English
Web Page Settings Guide	2017H-EN1	English
Software Setup Guide	2017L-EN1	English
Troubleshooting	2017L-EN1	English
MX-FR59U Data Security Kit Operation Guide	EX1	English
MX-FR59U Data Security Kit Notice	1.0	English
How to set up MX-FR59U to be the "Protection Profile for Hardcopy Devices" compliant	V1.0	English

7 Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Information Technology Security Center Evaluation Department that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation for the assurance components in the CC Part 3 by using the evaluation methods prescribed in the CEM as well as for the assurance activities of the Conformance PP was conducted.

Details for evaluation activities were reported in the Evaluation Technical Report.

The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict for every work unit in the CEM and assurance activity.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2017-12 and concluded upon completion of the Evaluation Technical Report dated 2018-04. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Furthermore, the evaluator conducted the evaluator testing at the developer site on 2018-02.

7.4 IT Product Testing

The evaluator performed independent testing and penetration testing based on the vulnerability assessment to ensure that the security functions of the product are certainly executed.

7.4.1 Developer Testing

The developer testing is not included in the assurance requirements of this evaluation.

7.4.2 Evaluator Independent Testing

The evaluator conducted an independent testing (hereinafter referred to as "independent testing") to ensure that the security functions of the product are certainly executed based on the evidence presented during the evaluation.

The independent testing performed by the evaluator is explained as follows.

(1) Independent Testing Environment

Configurations for the independent testing are based on the operational environment of the TOE shown in Figure 4-1, and the components are as shown in Table 7-1. Although there are differences in the following points, the evaluator also evaluates that these configurations are equivalent to the configuration identified in the ST, and there is no problem in checking the function of this TOE.

- The TOE tested by the evaluator is the case where the MFD main unit is MX-B355W or MX-B455W among the TOE Configuration indicated in the TOE Identification in Chapter 2 (see Table 2-1). The difference of the MFD main unit includes the printing speed (high / low) and the display language according to destination (English / Japanese). None of them affect security. However, in order to confirm that it does not affect the security functions, MX-B355W (printing speed: low, language: English) and MX-B455W (printing speed: high, language: Japanese) were tested.
- Firewalls installed to protect the TOE against unauthorized access from the external network do not exist in the testing environment because they do not affect the operation of the TOE.
- The evaluator used a telephone line simulator (a pseudo exchanger), which can emulate the same fax communication protocol as the PSTN, as an alternative to the PSTN.
- In the TLS test, communication between the TOE and the server / client PC is performed via the TLS testing tool created by the Evaluation Facility. Since the TLS testing tool only modifies the packet data of the TLS handshake message, it does not affect the functions of the TOE.
- For some tests such as cryptographic tests, the testing firmware created by the developer is used for calling for testing the cryptographic modules in the TOE.

The module called in the test using the testing firmware is the same as the module of the TOE, so it does not affect the functions of the TOE.

Table 7-1 Components of Independent Testing

Configuration Item	Detail
TOE	MX-B355W ・Option: MX-FR59U MX-B455W ・Option: MX-FR59U
Audit Server	rsyslog ver.8.24.0
Mail Server	Postfix ver.2.10.1
Authentication Server	openLDAP ver.2.4.44
FTP Server	Microsoft Internet Information Services ver.8.5 9600.16384
Client PC	OS : Windows 8.1 / 10 Web browser: ・Internet Explorer 11 ・Google Chrome 63.0.3239.132 Printer driver: ・SHARP MX-B355W PCL6 Driver 07.01.06.19 ・SHARP MX-B455W SPDL2 Driver 07.01.06.19

(2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

The viewpoints of the independent testing devised by the evaluator based on the assurance activities of the Conformance PP and on the evaluation documentation submitted for evaluation are shown below.

<Independent Testing Viewpoints>

1. Checking security functions by SFR.
2. Checking if the encryption implementation is correct.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

For the external interfaces of the TOE, inputs were provided using the TOE operation panel, client PC and testing tools, and the behaviors were observed using the following methods.

・ If the behavior can be observed from the external interface of the TOE, the external interface of the TOE is used.

・ If the behavior cannot be observed from the external interface of the TOE, the logs in the audit server are investigated, and network analyzer or testing firmware is used.

<Content of the Performed Independent Testing>

The independent testing was performed on 35 items by the evaluator.

Table 7-2 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 7-2 Content of the Performed Independent Testing

Viewpoint	Outline of the Independent Testing
1	Checking security functions ・To confirm for each SFR that all the security functions are as specified by the test items created from the assurance activities of the Conformance PP or the specification of SFR.
2	Checking encryption implementation ・To confirm the implementation of the following encryption algorithm to be tested by the testing firmware installed on the TOE. - RSA (key generation, signature generation/verification) - AES-CBC-128, AES-CBC-256, AES-ECB-256 - SHA-1, SHA-256 - HMAC-SHA-1, HMAC-SHA-256 - CTR_DRBG ・The encryption key of the user document data and the user document data encrypted and stored inside the TOE are taken out by the testing firmware and decrypted by the decryption tool to confirm that it is correctly encrypted.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation.

The penetration testing performed by the evaluator is explained as follows.

(1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

1. There is concern that it can be exploited by the fact that the unintended port of the TOE is enabled or a publicly known vulnerability exists in the running network service.
2. In the TOE web interface, there is concern that it can be exploited by the existence of publicly known vulnerabilities, such as bypass of the identification and authentication function by direct designation of URL, and XSS.
3. There is concern that manipulation of print job, buffer overflow or arbitrary code execution may occur due to unauthorized print data input to the TOE.
4. There is concern that the identification and authentication function may be bypassed due to unauthorized input from the operation panel, printer driver and web interface.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The following testing tools shown in the Table 7-3 below were added to the environment of the evaluator independent testing to implement.

Table 7-3 Penetration Testing Tools

Tool Name	Outline and Purpose of Use
Port Scan Tool nmap 7.60	It is used for searching ports.
Vulnerability Scan Tool Nessus 6.11.1	It is used for detecting publicly known vulnerability.
Web Vulnerability Scan Tool OWASP ZAP 2.7.0	It is used for detecting general vulnerability of web.
Web Application Analysis Tool Fiddler 5.0.20173.50948	It is used for capturing or issuing communication data received or sent by web application.
Printer Security Testing Tool PRET 0.39	It is used for detecting vulnerability of printing device by using printer language.
TCP/UDP Data Communication Tool Netcat 1.12	It is used for detecting vulnerability of identification and authentication.
Penetration Testing Tool Metasploit Framework v4.6.2	It is used for creating unauthorized print files.

<Content of the Performed Penetration Testing>

Table 7-4 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-4 Content of the Performed Penetration Testing

Vulnerability	Penetration Testing Outline
1	It is confirmed that unexpected ports are not open and that there is no publicly known vulnerability in the available ports by using the port scan tool and the vulnerability scan tool.
2	It is confirmed that there is no publicly known vulnerability in the Web interface by using the web vulnerability scan tool and web application analysis tool.
3	It is confirmed that unintended behavior does not occur by using print data in Postscript, PJL language, TIFF format and PDF format that are intended to generate unauthorized behavior.
4	It is confirmed that no unauthorized behavior occurs due to character strings entered in the identification and authentication function.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

The requirements of the TOE configurations, which are the assumptions for this evaluation, are as described in the guidance documents listed in Chapter 6. In order to enable the security functions of this TOE and use them securely, the TOE must be set as

described in the guidance documents. Different settings are not subject to assurance by this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM and all assurance activities in the Conformance PP by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:

  Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015

  Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

8 Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. The submitted documentation was sampled, the content was examined, and the related work units or assurance activities shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the method indicated in the CEM and in the assurance activities.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report and related evaluation documentation, the Certification Body determined that the TOE satisfies the following assurance components in the CC Part 3 and the assurance activities of the Conformance PP.

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer to "4.3 Clarification of Scope" and "7.5 Evaluated Configuration" to make sure that the scope of the evaluation target and operational requirements of the TOE meet the operational conditions they assume.

The audit data generated by the TOE is encrypted and stored in the TOE until it is successfully transmitted to the audit server. It is possible to store 40,000 audit data in the TOE. Newly generated audit data exceeding 40,000 are deleted. If the transmission to the audit server fails, the TOE tries to retransmit, but the operator needs to be careful about the warning messages displayed on the operation panel and the web page.

9 Annexes

There is no annex.

10 Security Target

The Security Target [12] of the TOE is provided as a separate document from this Certification Report.

Title:	MX-B455W / B355W with MX-FR59U Security Target
Version:	1.02
Publication Date:	2018-01-18
ST Author:	SHARP CORPORATION

11 Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
FTP	File Transfer Protocol
HCD	Hardcopy Device
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL/TLS
IPP	Internet Printing Protocol
LDAP	Lightweight Directory Access Protocol
MFD	Multifunction Device
NVS	Nonvolatile Storage
PSTN	Public Switched Telephone Network
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
XSS	Cross Site Scripting

The definitions of terms used in this report are listed below.

Field Replaceable (Unit)	The smallest subassembly that can be swapped in the field to repair a fault.
Hardcopy Device	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones" and other similar products.

12 Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

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

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] MX-B455W / B355W with MX-FR59U Security Target, Version 1.02, 2018-01-18, SHARP CORPORATION

[13] SHARP CORPORATION MX-B455W / B355W with MX-FR59U Evaluation Technical Report, Version 1.1, 2018-04-04, Information Technology Security Center Evaluation Department

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017