Ärendetyp: 6
Diarienummer: 19FMV3559-50:1
Dokument ID 7DFAYPHQVZ4V-1834444990-2007

Swedish Certification Body for IT Security

Certification Report - KYOCERA ECOSYS M3860idnf, ECOSYS M3860idnfG, TA Tri-umph-Adler/UTAX P-6038if MFP, with HDD

Issue: 1.0, 2020-maj-25

Authorisation: Ulf Noring, Lead Certifier , CSEC

Table of Contents

1 Executive Summary 3

2 Identification 5

3 Security Policy 6
3.1 User Management 6
3.2 Data Access 6
3.3 FAX Data Flow Control 6
3.4 Hard Disk Drive Encryption 6
3.5 Overwrite-Erase Function 6
3.6 Security Management 6
3.7 Network Protection 7

4 Assumptions and Clarification of Scope 8
4.1 Usage Assumptions 8
4.2 Clarification of Scope 8

5 Architectural Information 10
5.1 Physical Configuration of the TOE 10
5.2 Logical Configuration of the TOE 11

6 Documentation 12

7 IT Product Testing 13
7.1 Developer Testing 13
7.2 Evaluator Testing 13
7.3 Penetration Testing 14

8 Evaluated Configuration 15
8.1 Dependencies to Other Hardware, Firmware and Software 15
8.2 Excluded from the TOE Evaluated Configuration 15

9 Results of the Evaluation 16

10 Evaluator Comments and Recommendations 17

11 Glossary 18

12 Bibliography 19
12.1 General 19
12.2 Documentation 19

Appendix A Scheme Versions 21
A.1 Scheme/Quality Management System 21
A.2 Scheme Notes 21

1 Executive Summary

The Target of Evaluation (TOE) consists of the hardware and firmware of the following multifunction printer (MFP) models with Hard Disk:

KYOCERA:
ECOSYS M3860idnf
ECOSYS M3860idnfG

TA Triumph-Adler:
P-6038if MFP

UTAX:
P-6038if MFP

The TSF and its execution environment are the same in all the listed models above. The only difference between them are sales destinations. The following firmware is used by the system:

System firmware: 2WF_S0IS.C01.011

The above models provide copying, scanning, printing, faxing and box functionality.

The evaluated security features include user management, data access control, fax data flow control, job authorization, hard drive encryption, overwrite-erase functionality, security management, and network protection (IPSec and TLS).

The following functionality is excluded from the evaluation:
- The maintenance interface
- Network authentication
- The installation of Java applications on the MFP

The TOE is delivered to the customer by a courier trusted by KYOCERA Document Solutions Inc. The main MFP printer unit is delivered separately from the HDD add-on. The TOE can be purchased from a KYOCERA Document Solutions Inc. group corporation directly or from a dealer. A service person from the organisation that sold the TOE will set it up for the customer.

The evaluation has been performed by Combitech AB in their premises in Sundbyberg and Bromma, Sweden with testing done in the developer's premises in Osaka, Japan and was completed on the 20th of April, 2020.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 5, and the Common Methodology for IT Security Evaluation, version 3.1, revision 5. The evaluation conforms to evaluation assurance level EAL 2, augmented by ALC_FLR.2. The evaluation does not claim conformance to any Protection Profile.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Critera Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025:2018 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST] and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for the evaluation assurance level EAL 2 + ALC_FLR.2.

The technical information in this report is based on the Security Target [ST] and the Final Evaluation Report [FER] produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2019007
Name and version of the certified IT product	KYOCERA ECOSYS M3860idnf, ECOSYS M3860idnfG TA Triumph-Adler P-6038if MFP UTAX P-6038if MFP The HDD option HD-14 for the above printer models System Firmware: 2WF_S0IS.C01.011
Security Target Identification	ECOSYS M3860idnf Series with HDD Security Target
EAL	EAL 2 + ALC_FLR.2
Sponsor	Kyocera Document Solutions Inc.
Developer	Kyocera Document Solutions Inc.
ITSEF	Combitech AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	1.23.1
Scheme Notes Release	14.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2020-05-26

3 Security Policy

The TOE consists of seven security functions, listed below together with a short description of each function.Summary of the security services the TOE provides.

3.1 User Management

Identifies and authenticates whether persons are authorized users when users intend to operate the TOE from the operation panel or client PCs. When the TOE is used from the Operation Panel or a Web browser, the login screen is displayed and a user is required to enter his or her login user name and login password. When the TOE is accessed from the printer driver or TWAIN driver, the TOE identifies and authenticates if the person is authorized by referring to the login user name and login user password obtained from the job sent by the user. If the logon procedure fails consecutively for a certain amount of times, the user is locked out of their account for an amount of time set by the administrator. Users are automatically logged out after a certain period of inactivity.

3.2 Data Access

Allows authorized users to only access their own image and job data stored in the

TOE using each of the TOE basic function such as copy, scan to send, print, fax and box function. Users who own boxes can give other users permission to view the contents of a particular box, and also set a password to further protect the box.

3.3 FAX Data Flow Control

Makes sure that data received on the fax line interface is forwarded on to the internal network that the TOE is connected to.

3.4 Hard Disk Drive Encryption

A function that encrypts information assets stored in the HDD in order to prevent leakage of data stored in the HDD inside the TOE.

3.5 Overwrite-Erase Function

After each basic function (such as scanning, printing, etc.) completes, the TOE deletes used image data on the HDD or flash memory. When deleting stored image data on the HDD, the overwrite-erase function overwrites the actual image data with meaningless character strings so that it disables re-usage of the data.

3.6 Security Management

The security management function allows only authorized users to edit user information, set the TOE security functions, and manage TSF. The Security management function can be performed from the Operation Panel and Client PCs. A web browser is used for operation from Client PCs.

3.7 Network Protection

The network protection function verifies the propriety of the destination to connect to and protects targeted information assets against leaking and altering by applying encryption when using the Scan to Send Function, Print Function, Box Function, the Box Function from a Client PC (web browser), or the Security Management Function from a Client PC (web browser). Communication with a computer directly connected with the MFP is not encrypted.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes four assumptions on the usage of the TOE.

A.ACCESS

The hardware and software that the TOE is composed of are located in a protected environment from security invasion such as illegal analysis and alteration.

A.NETWORK

The TOE is connected to the internal network that is protected from illegal access from the external network.

A.USER_EDUCATION

The TOE users are aware of the security policies and procedures of their organization, and are educated to follow those policies and procedures.

A.DADMIN_TRUST

The TOE's administrators are competent to manage devices properly as a device administrator and have a reliability not to use their privileged access rights for malicious purposes.

4.2 Clarification of Scope

The Security Target contains three threats which have been considered during the evaluation.

T.SETTING_DATA

Malicious person may have unauthorized access to, to change, or to leak TOE setting data via the operation panel or client PCs.

T.IMAGE_DATA

Malicious person may illegally access not authorized box document data via the operation panel or Client PC and leak or alter them.

T.NETWORK

Malicious person may illegally eavesdrop or alter document data or TOE setting data on the internal network.

The Security Target contains three Organisational Security Policies (OSPs) which have been considered during the evaluation.

P.HDD_ENCRYPTION

TOE must encrypt document data and TOE setting data stored on HDD.

P.DOC_OVERWRITE

TOE must entirely overwrite and erases the actual data area, not only logically delete the management information of document data so that it disables re-usage of the data where document data that was created on the HDD during usage of the basic functions of the TOE.

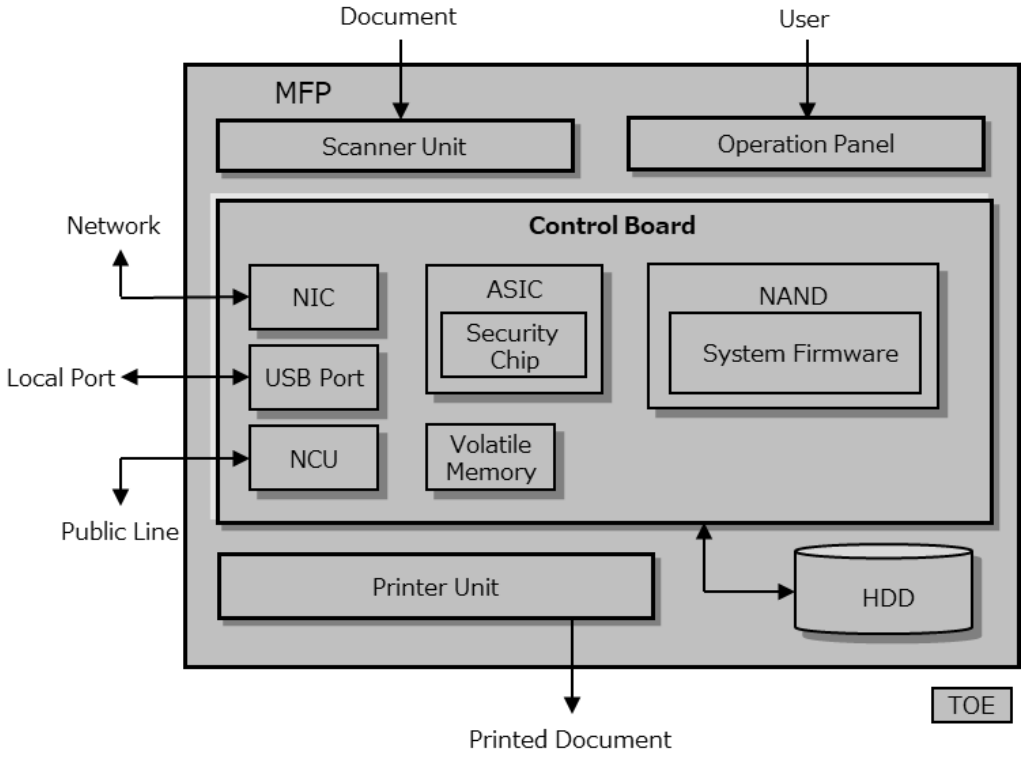
P.FAX_CONTROL

TOE must control not to forward the data received from a public line to the internal network that the TOE is connected.

5 Architectural Information

5.1 Physical Configuration of the TOE

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Control Board, a hard disk drive (HDD), the system firmware, and the guidance documents. The different parts (except for the guidance documentation) are depicted in the diagram below.



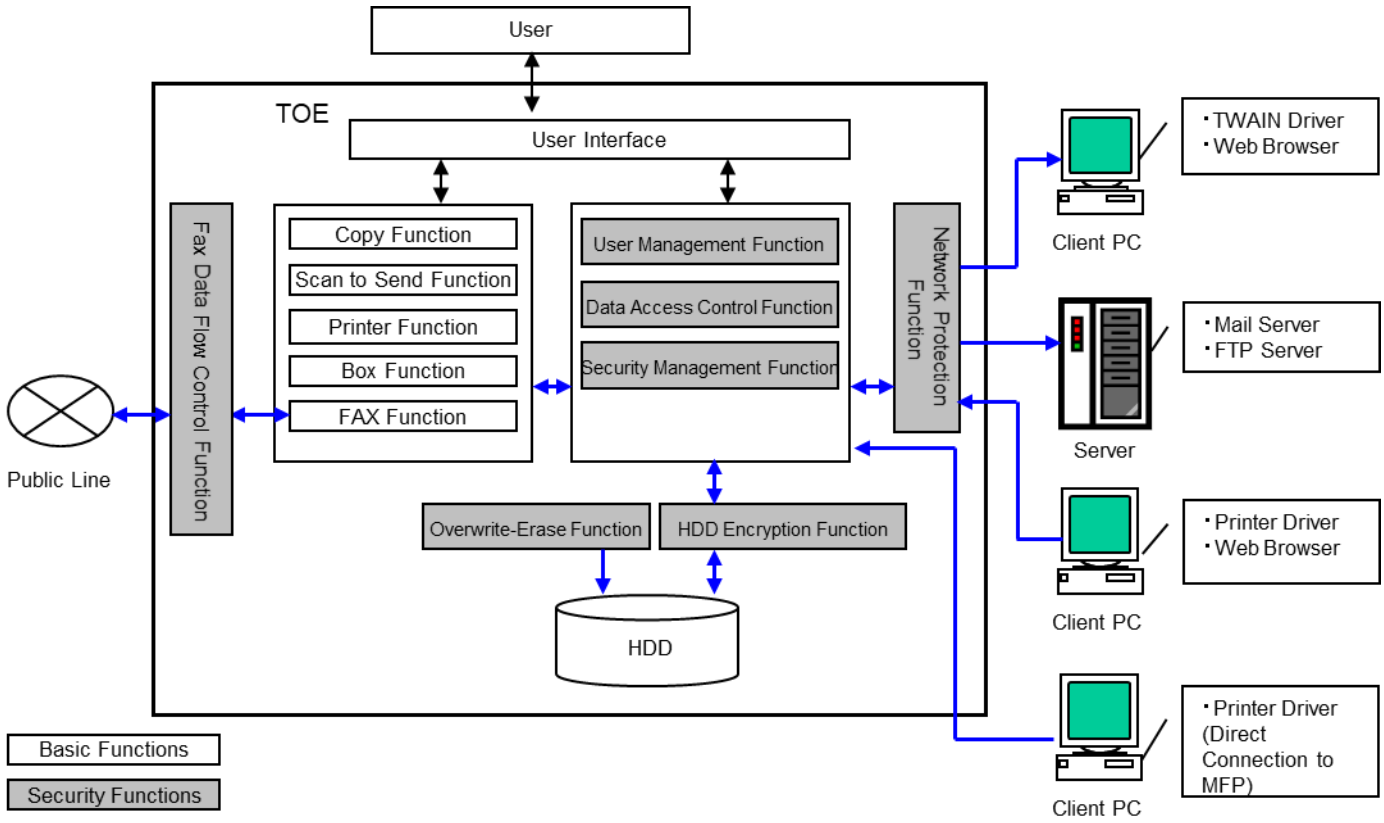
The Operation Panel is the hardware that displays status and results upon receipt of input by the TOE user. The Scanner and Printer units are the hardware that input documents into the TOE and output documents as printed material.

The Control Board is the circuit board that controls the entire TOE. A system firmware is installed on a NAND which is positioned on the Control Board. The Control Board has a Network Interface (NIC), a Local Interface (USB Port), and a Public Line for sending and receiving faxes (NCU). There is also an ASIC on the Main Board. The ASIC includes a Security Chip which implements security arithmetic processing for the HDD encryption function and HDD Overwrite-Erase function.

The NAND stores device settings while the Volatile Memory is used as a working area. The HDD that stores image data and job data is connected to the Control Board. Any of the above memory mediums are not removable. Device setting data related to Box functionality is stored in the HDD.

5.2 Logical Configuration of the TOE

The below diagram illustrates the logical scope of the TOE:



Please see section 1.4.3 in the [ST] for a more detailed description of the functionality shown in the diagram. There is no interface for any user or administrator to directly interact with the TOE operating system, all interactions must be made via one of the standard application functions or the hardware interfaces of the TOE.

6 Documentation

The following guidance documents are available:

[NOTICE]
Notice

[QG]
ECOSYS M3860idnf / ECOSYS M3860idn First Steps Quick Guide

[OG]
ECOSYS M3860idnf / ECOSYS M3860idn Operation Guide

[SG]
ECOSYS M3860idnf / ECOSYS M3860idn Safety Guide

[OG-FAX]
ECOSYS M3860idnf / ECOSYS M3860idn FAX Operation Guide

[OG-DE]
Data Encryption/Overwrite Operation Guide

[UG-CCRX]
Command Center RX User Guide

[UG-PD]
ECOSYS M3860idnf / ECOSYS M3860idn Printer Driver User Guide

[UG-NDP]
KYOCERA Net Direct Print User Guide

7 IT Product Testing

7.1 Developer Testing

The developer performed extensive manual tests on the following printer models:

ECOSYS M3860idnf

Since the TSF and its execution environment are the same in the model listed above and the other TOE models listed in chapter 1, and the only differences between them are sales destinations, this covers all of the TOE models listed in chapter 1.

The developer testing was done on the following firmware:

2WF_S0IS.C01.011

The developer's testing covers the security functional behaviour of all TSFIs and most SFRs. Some gaps to the SFRs were identified and covered by evaluator independent testing. All test results were as expected. The testing was performed on the developer's premises in Osaka, Japan.

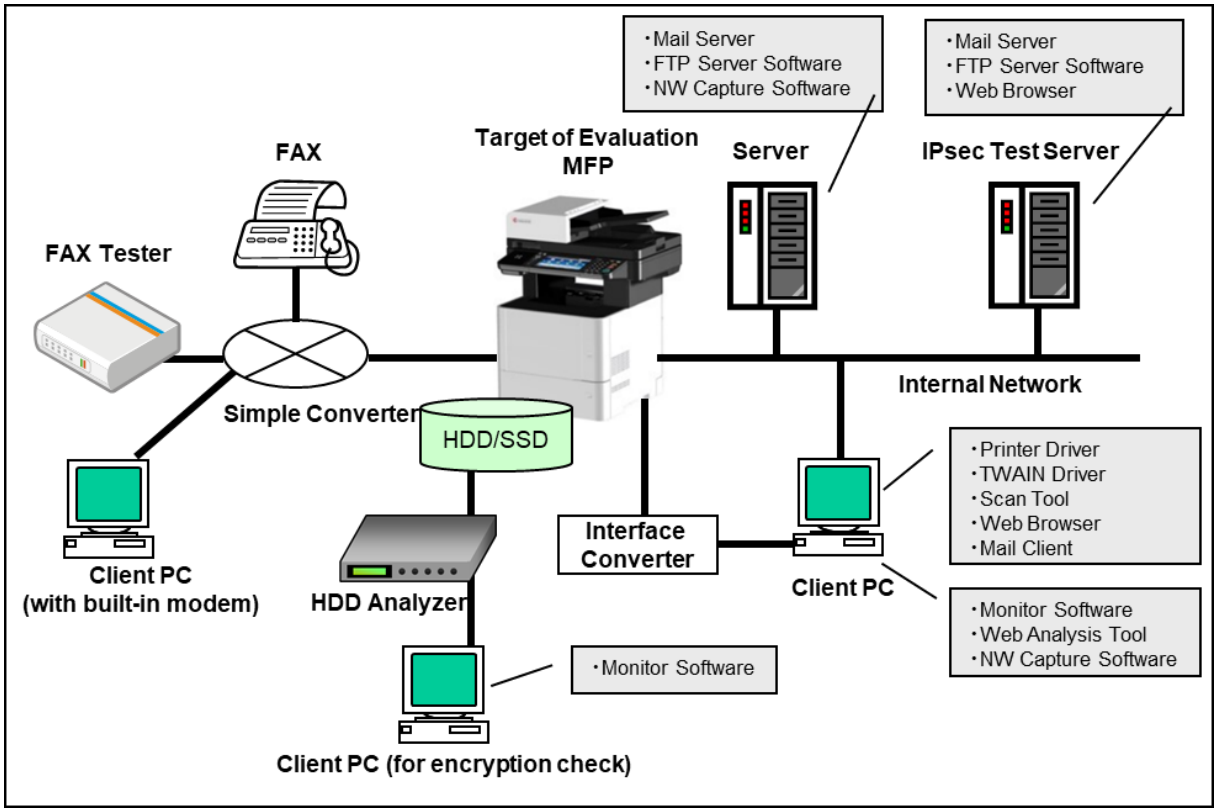
7.2 Evaluator Testing

The evaluator's independent tests were chosen to complement the developer's manual tests in order to complement the cover of the security functional behaviour of the SFRs. The evaluator repeated a sample of the developer's test cases and performed individual and penetration test cases. The tests included:

TOE Installation
Identification and Authentication
Data Access Control
Encryption/Overwrite-Erase
Security Management
Network Protection

7.2.1 Test Environment

The evaluator performed the tests on the developer's premises in Osaka, Japan using the same test environment as the developer. This was accepted since the only difference between the different TOE models is the sales destination. The test environment was set up according to the below diagram:



7.3 Penetration Testing

The evaluators penetration tested the TOE using the same test environment as described above in chapter 7.2.1. The following types of penetration tests were performed:

- Port scan
- Vulnerability scan including web application vulnerability scan
- JPG fuzzing
- TLS scanning

Port scans were run after installation and configuration had been done according the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned for TCP/UDP.

Nessus (www.tenable.com) basic network vulnerability scans were run. No high, medium, or low severity issues concerning the evaluated configuration were found.

A JPG picture were fuzzed approximate 110 times using the Peach fuzzing tool.

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

A notice [NOTICE] included with the TOE details verification procedures of the TOE, explains that use of applications on the TOE is not allowed in the evaluated configuration, and guides users to follow the Data Encryption/Overwrite Operation Guide [OG-DE] to configure the TOE. The Data Encryption/Overwrite Operation Guide [OG-DE] describes how to configure the TOE to reach evaluated configuration in the chapter named "Installing the Security Functions", in the subchapter "After Installation". The instructions need to be followed in order to use the evaluated configuration.

8.1 Dependencies to Other Hardware, Firmware and Software

The TOE is the hardware and firmware of the various MFP models listed in chapter 1 as well as the guidance needed to configure and operate the TOE.

To be fully operational, any combination of the following items may be connected to the MFP:

- A LAN for network connectivity.
- A telephone line for fax capability.
- IT systems that submit print jobs to the TOE via the network using standard print protocols.
- IT systems that send/and or receive faxes via the telephone line
- An SMTP server/FTP server/client PC/other FAX system/USB memory that will receive any input sent to the MFP if the MFP is configured to send it to them.
- A USB memory that can be used as an input source for print jobs (i.e. print from USB), or to copy documents to from a box.

8.2 Excluded from the TOE Evaluated Configuration

The following features of the TOE are outside of the evaluated configuration:

- The maintenance interface
- Networked user authentication such as LDAP

Expanding functionality by installing Java applications is not allowed in the TOE evaluated configuration. The user manual [OG] calls the Java applications "applications". More information can be found in chapter 5-11, "Application", in [OG].

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.2	PASS
Parts of the TOE CM Coverage	ALC_CMS.2	PASS
Delivery procedures	ALC_DEL.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.2	PASS
Basic design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CM	Configuration Management
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within an evaluation and certification scheme
LAN	Local Area Network
MFP	Multi-Function Printer
NCU	Network Control Unit
OSP	Organizational Security Policy
PP	Protection Profile
SMTP	Simple Mail Transport Protocol
SSD	Solid State Disk
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

12 Bibliography

12.1 General

CCp1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001
CCp2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002
CCp3	Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004
ST	ECOSYS M3860idnf Series with HDD Security Target, KYOCERA Document Solutions Inc., 2019-03-31, document version 1.02
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2019-09-25, document version 9.0

12.2 Documentation

NOTICE	Notice, ECOSYS M3860idnf, ECOSYS M3860idnfG, P-6038if MFP, KYOCERA Document Solutions Inc., 2020-01, document version 303MS5641003
QG	FIRST STEPS QUICK GUIDE, ECOSYS 3860idnf, ECOSYS M3860idn, KYOCERA Document Solutions Inc., 2019-04, document version 3V2WF5601001
OG	OPERATION GUIDE, ECOSYS 3860idnf, ECOSYS M3860idn, KYOCERA Document Solutions Inc., 2019-04, document version 2WDFDEN000
SG	ECOSYS M3860idnf / ECOSYS M3860idn Safety Guide, KYOCERA Document Solutions Inc., 2019-04, document version 3V2WF5621001
OG-FAX	FAX Operation Guide, ECOSYS 3860idnf, ECOSYS M3860idn, KYOCERA Document Solutions Inc., 2019-04, document version 2WFKDEN500
OG-DE	Data Encryption/Overwrite, Operation Guide, ECOSYS M3860idnf, ECOSYS M3860idn, KYOCERA Document Solutions Inc., 2019-11,

document version 3MT2WFKDEN003

UG-CCRX Command Center RX, User Guide, KYOCERA Document Solutions Inc., 2017-10, document version CCRXKDEN13

UG-PD Printer Driver, User Guide, ECOSYS 3860idnf, ECOSYS M3860idn, KYOCERA Document Solutions Inc., 2019-04, document version 2WFBWKDEN740

UG-NDP KYOCERA Net Direct Print, User Guide, KYOCERA Document Solutions Inc., 2019-02, document version DirectPrintKDEN2.2019.02

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.23.1	2020-03-06	None
1.23	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL2: evaluator + developer tests together provide full coverage of the TSFI.
SN-18	1.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	1.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.