Swedish Certification Body for IT Security

Certification Report - Kyocera TASKalfa MZ4000i, MZ3200i 2600PP

Issue: 1.0, 2023-mar-16

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Accred. no. 1917
Certification of Products
ISO/IEC 17065

SWEDAC ACKREDITERING
Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary 3

2 Identification 5

3 Security Policy 6
3.1 User Management 6
3.2 Data Access Control 6
3.3 Job Authorization 6
3.4 HDD Encryption 7
3.5 Overwrite-Erase 7
3.6 Audit Log 7
3.7 Security Management 7
3.8 Self-Test 7
3.9 Network Protection 7

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

5 Architectural Information 10

6 Documentation 11

7 IT Product Testing 12
7.1 Developer Testing 12
7.2 Evaluator Testing 12
7.3 Penetration Testing 12

8 Evaluated Configuration 13

9 Results of the Evaluation 14

10 Evaluator Comments and Recommendations 15

11 Glossary 16

12 Bibliography 17

Appendix A Scheme Versions 19
A.1 Quality Management System 19
A.2 Applicable Scheme Notes 19

1 Executive Summary

The TOE is the hardware and the firmware of the following multifunction printer (MFP) models with hard disk and with FAX:

KYOCERA TASKalfa MZ4000i, MZ3200i, M30040i and M30032i

Copystar CS MZ4000i and CS MZ3200i

TA Triumph-Adler 4063i and 3263i

UTAX 4063i and 3263i

with the following firmware:

System firmware 2ZS_S0IS.C02.504

FAX firmware 3R2_5100.003.012

In the evaluated configuration, the hard disk HD-15 and FAX System 12 are installed and included in the scope of the TOE.

The TOE provides copying, scanning, printing, faxing and boxing (storage).

Delivery is done by means of a courier trusted by KYOCERA Document Solutions Inc. Installation and initial setup is done by a representative of KYOCERA or the approved reseller.

The ST claims demonstrable conformance to the Protection Profile (PP):

IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20) ([PP2600.2]) v1.0, including the PRT, SCN, CPY, FAX, DSR and SMI packages, in accordance with NIAP CCEVS Policy Letter #20.

The evaluation has been performed by Combitech AB, in their premises in Växjö and Bromma, Sweden, and was completed on the 4th of March 2023.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 revision 5, and Common Evaluation Methodology (CEM), version 3.1 revision 5.

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

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 the Common Methodology for evaluation assurance level EAL 2 augmented by 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	CSEC2022005
Name and version of the certified IT product	KYOCERA TASKalfa MZ4000i, TASKalfa MZ3200i, TASKalfa M30040i, TASKalfa M30032i, Copystar CS MZ4000i, CS MZ3200i, TA Triumph-Adler 4063i, 3263i UTAX 4063i, 3263i with Hard Disk and FAX System, all with system firmware: 2ZS_SOIS.C02.504 and fax firmware: 3R2_5100.003.012
Security Target Identification	TASKalfa MZ4000i, TASKalfa MZ3200i Series with Hard Disk and FAX System Security Target
EAL	EAL 2 + ALC_FLR.2
PP claims	Demonstrable conformance to IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" v1.0 (with NIAP CCEVS Policy Letter #20)
Sponsor	Kyocera Document Solutions Inc.
Developer	Kyocera Document Solutions Inc.
ITSEF	Combitech AB
Common Criteria version	3.1 release
CEM version	3.1 release
QMS version	2.3
Scheme Notes Release	20.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2023-03-16

3 Security Policy

TOE provides the following security services:

- User Management
- Data Access Control
- Job Authorization
- HDD Encryption
- Overwrite-Erase
- Audit Log
- Security Management
- Self-Test
- Network Protection

3.1 User Management

A function that identifies and authenticates users so that only authorized users can use the TOE. When using the TOE from the Operation Panel and Client PCs, a user will be required to enter his/her login user name and login user password for identification and authentication. The User Management Function includes a User Account Lockout Function, which prohibits the users access for a certain period of time if the number of identification and authentication attempts consecutively result in failure, a function, which protects feedback on input of login user password when performing identification and authentication and a function, which automatically logouts in case no operation has been done for a certain period of time.

3.2 Data Access Control

A function that restricts access to protected assets so that only authorized users can access to the protected assets inside the TOE.

The following types of Access Control Functions are available.

- Access Control Function to control access to image data
- Access Control Function to control access to job data

3.3 Job Authorization

A function that restricts usage of the function so that only authorized persons can use basic functions of the TOE .

The following types of Job Authorization are available.

- Copy Job (Copy Function)
- Print Job (Print Function)
- Send Job (Scan to Send Function)
- FAX Send Job (FAX Function)
- FAX Reception Job (FAX Function)
- Storing Job (Box Function)
- Network Job (Network Protection Function)

3.4 HDD 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

A function that does not only logically delete the management information of the image data, but also entirely overwrites and erases the actual data area so that it disables re-usage of the data where image data that was created on the HDD or the Flash Memory during usage of the basic functions of the TOE.

3.6 Audit Log

A function that records and stores the audit logs of user operations and security-relevant events on the HDD. This function provides the audit trails of TOE use and security-relevant events. Stored audit logs can be accessed only by a device administrator. The stored audit logs will be sent by email to the destination set by the device administrator.

3.7 Security Management

A function that sets security functions of the TOE. This function can be used only by authorized users. This function can be utilized from an Operation Panel and a Client PC. Operations from a Client PC use a web browser.

3.8 Self-Test

A function that verifies the integrity of TSF executable code and TSF data to detect unauthorized alteration of the executable code of the TOE security functions.

3.9 Network Protection

A function that protects communication paths to prevent leaking and altering of data by eavesdropping of data in transition over the internal network connected to TOE.

This function verifies the propriety of the destination to connect to and protects targeted information assets by encryption, when using a Scan to Send Function, a Print Function, a Box Function and a BOX Function from a Client PC (web browser), or a Security Management Function from a Client PC (web browser). However, usage of a Print Function directly connected to a MFP is exception.

This function also provides a feature to prevent forwarding of information from an external interface to an internal network through TOE without permission.

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

A.ACCESS.MANAGED

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.USER.TRAINING

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.ADMIN.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 correctly configure and operate the TOE in accordance with those policies and procedures.

A.ADMIN.TRUST

Administrators do not use their privileged access rights for malicious purposes.

4.2 Clarification of Scope

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

T.DOC.DIS

User Document Data may be disclosed to unauthorized persons

T.DOC.ALT

User Document Data may be altered by unauthorized persons

T.FUNC.ALT

User Function Data may be altered by unauthorized persons

T.PROT.ALT

TSF Protected Data may be altered by unauthorized persons

T.CONF.DIS

TSF Confidential Data may be disclosed to unauthorized persons

T.CONF.ALT

TSF Confidential Data may be altered by unauthorized persons

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

P.USER.AUTHORIZATION

To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.

P.SOFTWARE.VERIFICATION

To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

P.AUDIT.LOGGING

To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.

P.INTERFACE.MANAGEMENT

To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

P.HDD.ENCRYPTION

To improve the confidentiality of the documents, User Data and TSF Data stored in HDD will be encrypted by the TOE.

5 Architectural Information

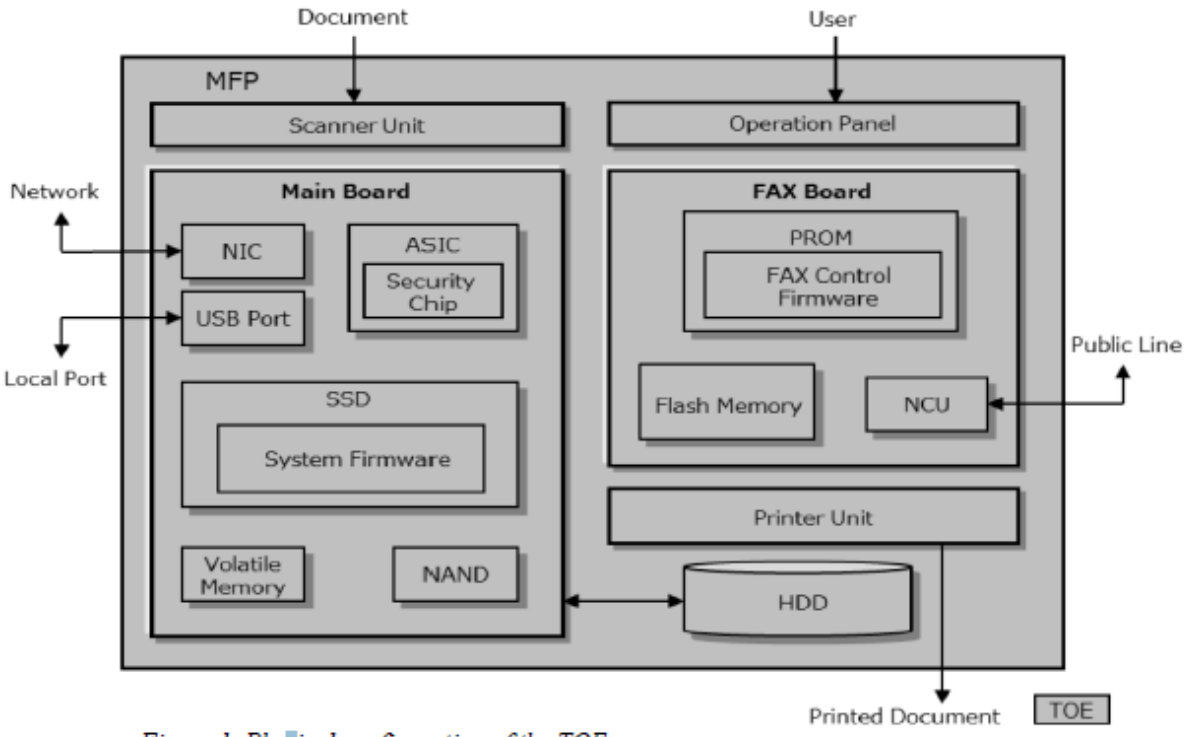

Figure 1, Physical configuration of the TOE

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Main Board, a FAX Board, HDD and SSD hardware, and some firmware.

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

A Main Board is the circuit board to control entire TOE. A system firmware is installed on a SSD, which is positioned on the Main Board. The Main Board has a Network Interface (NIC) and a Local Interface (USB Port).

The ASIC that is also on the Main Board includes a Security Chip, which shares installation of some of the security functions. The Security Chip realizes security arithmetic processing for HDD encryption function and HDD Overwrite-Erase function

A FAX control firmware that controls FAX communication is installed on the PROM, which is positioned on the FAX Board. Additionally, a FAX Board has a NCU (Network Control Unit) as an interface.

6 Documentation

For proper configuration into the evaluated configuration, the following guidance documents are available:

Notice1 (KYOCERA)
Notice2 (KYOCERA)
Notice3 (Copystar)
Notice4 (TA Triumph-Adler/UTAX)

FAX System 12 Installation Guide

TASKalfa MZ4000i / TASKalfa MZ3200i First Steps Quick Guide

TASKalfa MZ4000i / TASKalfa MZ3200i Operation Guide

TASKalfa MZ4000i / TASKalfa MZ3200i Safety Guide

FAX System 12 Operation Guide

Data Encryption/Overwrite Operation Guide

Command Center RX User Guide

TASKalfa MZ4000i / TASKalfa MZ3200i Printer Driver User Guide

KYOCERA Net Direct Print User Guide

7 IT Product Testing

7.1 Developer Testing

The developer performed extensive testing with good coverage of the TSFI on the TASKalfa MZ4000i and the TASKalfa MZ3200i models, with

System Firmware 2ZS_S0IS.C02.504

FAX Firmware 3R2_5100.003.012

Each of the other models are functionally identical to one of the tested models.

The developer testing was performed in the developer's premises in Osaka, Japan.

All test results were as expected.

7.2 Evaluator Testing

The evaluators' testing was performed in the evaluator's premises in Växjö, Sweden, between 2022-11-08 and 2022-11-13. The MX3200i model was used.

More than 50% of the developer tests were repeated. Some complementary tests were run as well.

All test results were as expected.

7.3 Penetration Testing

The evaluator penetration testing was performed in the evaluator's premises in Växjö, Sweden, between 2022-11-08 and 2022-11-13. The MX3200i model was used.

NMAP was used to perform a series of port scans, NESSUS was used for a vulnerability scan, and Peach fuzzer was used for jpeg fuzzing. Also, some negative tests were performed as part of the independent testing.

No anomalies were encountered and all results were as expected.

8 Evaluated Configuration

In the TOE operational environment, the following non-TOE hardware, and software is expected:

Client PC with KX printer driver, Kyocera TWAIN driver, and web browser

Mail server connected via IPSec (IKE 1)

FTP server connected via IPSec (IKE 1)

Mandatory in the evaluated configuration:

- a hard disk HD-15 and a FAX System 12 faxboard shall be installed and are included in the scope of the TOE.
- maintenance interfaces shall not be accessible

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 Cri-teria 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

ST — TASKalfa MZ4000i, TASKalfa MZ3200i Series with Hard Disk and FAX System Security Target, KYOCERA document solutions Inc., 2022-12-06, document version 1.00, FMV ID 22FMV4136-26

Notice2 — NoticeMZ (KYOCERA), Kyocera Document Solutions Inc., December 2022, document version 302ZS5641001, FMV ID 22FMV4136-8

Notice1 — NoticeM (KYOCERA), Kyocera Document Solutions Inc., December 2022, document version 302ZS5644001, FMV ID 22FMV4136-8

Notice3 — Notice3 (Copystar), Kyocera Document Solutions Inc., December 2022, document version 302ZS5642002, FMV ID 22FMV4136-8

Notice4 — Notice4 (TA Triumph-Adler/UTAX), Kyocera Document Solutions Inc., December 2022, document version 302ZS5643001, FMV ID 22FMV4136-8

IG-FAX — FAX System 12 Installation Guide, Kyocera Document Solutions Inc., September 2020, document version 303RK5671202, FMV ID 22FMV4136-8

QG — TASKalfa MZ4000i / TASKalfa MZ3200i First Steps Quick Guide, Kyocera Document Solutions Inc., November 2021, document version 302ZS5602001, FMV ID 22FMV4136-8

OG — TASKalfa MZ4000i / TASKalfa MZ3200i Operation Guide, Kyocera Document Solutions Inc., May 2022, document version 2ZSKDEN002, FMV ID 22FMV4136-8

SG — TASKalfa MZ4000i / TASKalfa MZ3200i Safety Guide, Kyocera Document Solutions Inc., November 2021, document version 302ZS5622001, FMV ID 22FMV4136-8

OG-FAX — FAX System 12 Operation Guide, Kyocera Document Solutions Inc., January 2022, document version 2ZSKDENCS500, FMV ID 22FMV4136-8

DE	Data Encryption/Overwrite Operation Guide, Kyocera Document Solutions Inc., September 2022, document version 3MS2ZSKDEN0, FMV ID 22FMV4136-8
CCRX	Command Center RX User Guide, Kyocera Document Solutions Inc., May 2022, document version CCRXKDEN28, FMV ID 22FMV4136-8
PD	TASKalfa MZ4000i / TASKalfa MZ3200i Printer Driver User Guide, Kyocera Document Solutions Inc.,May 2022, document version 02ZSBWKTEN821.2022.5, FMV ID 22FMV4136-8
NDP	KYOCERA Net Direct Print User Guide, Kyocera Document Solutions Inc., May 2022, document version DirectPrintKDEN3.2022.5, FMV ID 22FMV4136-8
PP2600B	2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B, IEEE, with NIAP CCEVS Policy Letter #20, June 2009, document version 1.0
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003
CC	CCpart1 + CCPart2 + CCPart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004
EP-002	EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0

Appendix A Scheme Versions

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

A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered 2022-05-19:

QMS 2.1.1	valid from 2022-03-09
QMS 2.2	valid from 2022-06-27
QMS 2.3	valid from 2023-01-26

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system. The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 2.3”.

The certifier concluded that, from QMS 2.1.1 to the current QMS 2.3, there are no changes with impact on the result of the certification.

A.2 Applicable Scheme Notes

SN-15 Testing

SN-18 Highlighted Requirements on the Security Target

SN-22 Vulnerability assessment

SN-27 ST requirements at the time of application for certification

SN-28 Updated procedures for application, evaluation and certification