Swedish Certification Body for IT Security

Certification Report Kyocera TASKalfa4 HCDPP

Issue: 1.0, 2023-okt-19

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the hardware and the firmware of the following multifunction printer (MFP) models with Hard Disk, FAX, and Data Security Kit:

Kyocera TASKalfa MZ4000i, MZ3200i, M30040i, M30032i.
Copystar CS MZ4000i, MZ3200i.
Triumph Adler 4063i, 3263i.
UTAX 4063i, 3263i.

with the following firmware:

System firmware 2ZS_S0IS.C02.504
FAX firmware 3R2_5100.003.012

In the evaluated configuration, the optional hard disk, the optional fax board and the optional data security kit are installed and included in the scope of the TOE.

The TOE provides copying, scanning, printing, faxing and boxing.

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.

The ST claims exact conformance to the Protection Profile for Hardcopy Devices (HCDPP) v1.0, including Errata #1

The evaluation has been performed by Combitech AB, in their premises in Växjö, Sweden, and was completed on the 3rd of October 2023.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 revision 5, Common Evaluation Methodology (CEM), version 3.1 revision 5, and the HCDPP v1.0 including Errata #1.

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), the Common Methodology for evaluation assurance level EAL 1 augmented by ASE_SPD.1, and the HCDPP v1.0 including Errata#1.

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

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	CSEC2022004
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, FAX System and Data Security Kit, system firmware 2ZS_S0IS.C02.504 and FAX firmware 3R2_5100.003.012
Security Target Identification	TASKalfa MZ4000i, TASKalfa MZ3200i Series with Hard Disk, FAX System and Data Security Kit Security Target
EAL	EAL 1 + ASE_SPD.1
PP claims	Exact conformance to the Protection Profile for Hardcopy Devices (HCDPP) v1.0, including Errata #1
Sponsor Developer ITSEF	KYOCERA document solutions Inc. KYOCERA document solutions Inc. Combitech AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	QMS 2.4.2
Scheme Notes Release	21.0
Recognition Scope	CCRA
Certification date	2023-10-19

3 Security Policy

The TOE provides the following security services:

- User Management
- Data Access Control
- Job Authorization
- HDD Encryption
- Overwrite-Erase
- Audit Log
- Security Management
- Trusted Operation
- Network Protection
- PSTN Fax-Network Separation

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)

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 send to Audit Log server 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.

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 Trusted Operation

A function that verifies the authenticity of the firmware when updating the firmware of TOE.

And 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).

3.10 PSTN Fax-Network Separation

The TOE ensures separation between the PSTN fax line and the Internal Network.

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.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 Clarification of Scope

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

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.

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.

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

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.

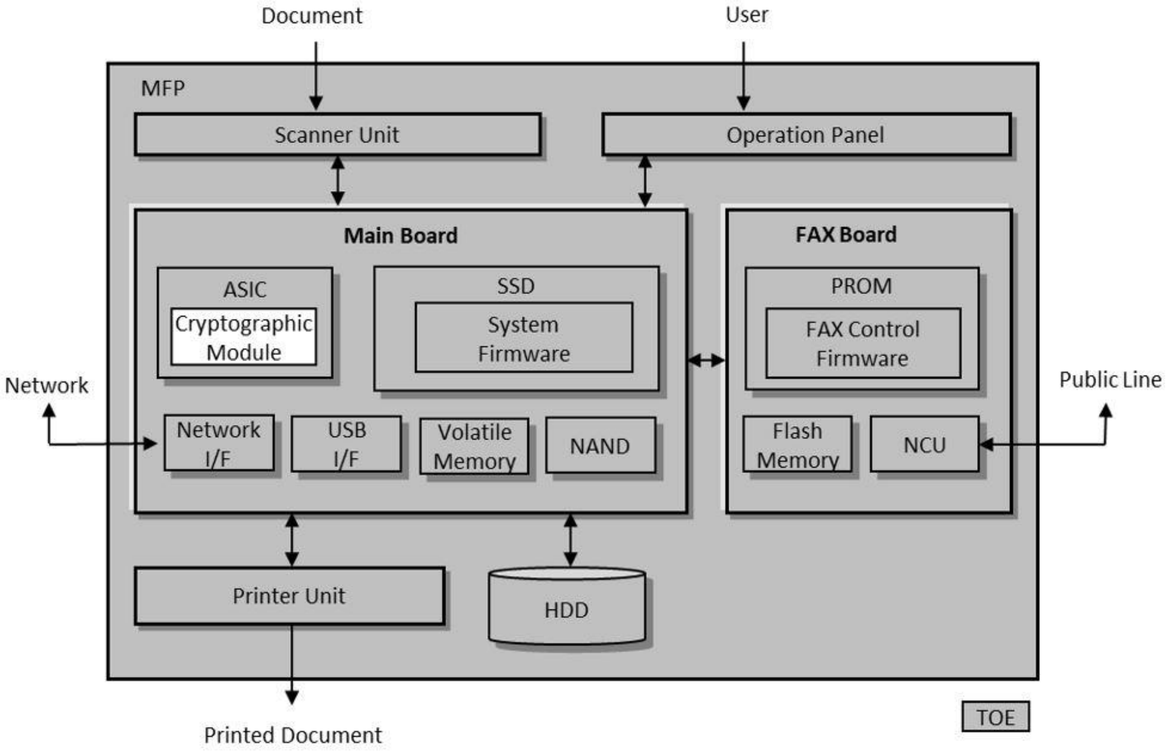
P.IMAGE_OVERWRITE

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.

5 Architectural Information



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

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 and a USB Interface.

The ASIC on the Main Board is installed with a cryptographic module to perform the HDD encryption function and Overwrite-Erase function. A FIPS 140-2 certified cryptographic module, key derivation and entropy are provided by this cryptographic module in TOE environment.

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 as an interface.

6 Documentation

The following guidance documents are part of the TOE:

Notice (KYOCERA) (302ZS5641001)

Notice (KYOCERA) (302ZS5644001)

Notice (Copystar)

Notice (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

7 IT Product Testing

7.1 Evaluator Testing

All TOE variants included in the evaluation use the same firmware and execute on the same main board with the same processor. The TASKalfa MZ3200i model was used for testing, representing all TOE variants.

All the test cases defined in the HCDPP were performed. The testing took place in Combitech's premises in Växjö, between 2023-04-21 and 2023-06-13.

All tests were successful and no errors were discovered.

7.2 Penetration Testing

The TASKalfa MZ3200i model was used for penetration testing.

The evaluators performed port scans (NMAP), vulnerability scan (Nessus), and jpeg fuzz tests (Peach).

The testing took place in Combitech's premises in Växjö, between 2023-06-01 and 2023-06-08

No vulnerabilities were found during the penetration testing.

8 Evaluated Configuration

In the evaluated configuration, the optional hard disk, the optional fax board and the optional data security kit are installed and included in the scope of the TOE.

The following features are excluded from the evaluated configuration:

- Maintenance Interface

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 securi-ty 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.1	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.1	PASS
CM Coverage	ALC_CMS.1	PASS
Development	ADV	PASS
Security-enforcing functional specification	ADV_FSP.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Independent testing	ATE_IND.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.1	PASS

The assurance activities in the HCDPP v1.0 including Errata #1 also have the verdict:	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

ST TASKalfa MZ4000i, TASKalfa MZ3200i Series with Hard Disk, FAX System and Data Security Kit Security Target, Kyocera Document Solutions Inc., 2022-11-11, document version 0.90

N1 Notice (KYOCERA), Kyocera Document Solutions Inc., December 2022, 302ZS5641001,

N2 Notice (KYOCERA), Kyocera Document Solutions Inc., December 2022, document version 302ZS5644001

N3 Notice (Copystar), Kyocera Document Solutions Inc., December 2022, document version 302ZS5642002

N4 Notice (TA Triumph-Adler/UTAX), Kyocera Document Solutions Inc., Kyocera Document Solutions Inc., December 2022, document version 302ZS5643001

IG-FAX FAX System 12 Installation Guide, Kyocera Document Solutions Inc., September 2020, document version 303RK5671202

QG TASKalfa MZ4000i / TASKalfa MZ3200i First Steps Quick Guide, Kyocera Document Solutions Inc., November 2021, document version 302ZS5602001

OG TASKalfa MZ4000i / TASKalfa MZ3200i Operation Guide, Kyocera Document Solutions Inc., May 2022, document version 2ZSKDEN002

SG TASKalfa MZ4000i / TASKalfa MZ3200i Safety Guide, Kyocera Document Solutions Inc., November 2021, document version 302ZS5622001

OG.FAX FAX System 12 Operation Guide, Kyocera Document Solutions Inc., January 2022, document version 2ZSKDENCS500

DE Data Encryption/Overwrite Operation Guide, Kyocera Document Solutions Inc., September 2022, document version 3MS2ZSKDEN0

CCRX Command Center RX User Guide, Kyocera Document Solutions Inc., May 2022, document version CCRXKDEN28

PD TASKalfa MZ4000i / TASKalfa MZ3200i Printer Driver User Guide, Kyocera Document Solutions Inc., May 2022, document version 02ZSBWKTEN821.2022.5

HCDPP Protection Profile for Harcopy Devices, IPA, NIAP and MFP Technical Community, 2015-09-10, document version 1.0, (including Errata #1, June 2017)

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

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
2.4.2	2023-09-20	None.
2.4.1	2023-09-20	None.
2.4	2023-06-15	None.
2.3.1	2023-04-20	None.
2.3	2023-01-26	None.
2.2	2022-06-27	None.
2.1.1	2022-03-09	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the certification:

SN 15 - Testing
SN 18 - Highlighted Requirements on the ST
SN 21 - NIAP PP Certifications
SN 22 - Vulnerability Assessment
SN 23 - Evaluation Reports for NIAP PPs and cPPs
SN 28 - Updated procedures