Swedish Certification Body for IT Security

Certification Report Kyocera TASKalfa MZ4001ci

Issue: 1.0, 2026-feb-26

Authorisation: Michael Lindh Almér, 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 FAX System:

- KYOCERA TASKalfa MZ7001ci
- KYOCERA TASKalfa MZ6001ci
- KYOCERA TASKalfa MZ5001ci
- KYOCERA TASKalfa MZ4001ci
- KYOCERA TASKalfa M30150ci
- KYOCERA TASKalfa M30140ci
- TA Triumph-Adler 7009ci
- TA Triumph-Adler 6009ci
- TA Triumph-Adler 5009ci
- TA Triumph-Adler 4009ci
- UTAX 7009ci
- UTAX 6009ci
- UTAX 5009ci
- UTAX 4009ci

With the system firmware C2G_S000.001.226 and FAX System 14.

In the evaluated configuration, the optional fax board is 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 evaluation has been performed by Combitech AB, in their premises in Bromma, Sweden, and was completed on the January 28, 2026.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 2022 and the Common Methodology (CEM) version 2022. The evaluation was performed at evaluation assurance level EAL 2, augmented by ALC_FLR.2.

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 2 augmented by ALC_FLR.2.

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	CSEC2024018
Name and version of the certified IT product	TASKalfa MZ7001ci, TASKalfa MZ6001ci, TASKalfa MZ5001ci, TASKalfa MZ4001ci, TASKalfa M30150ci, TASKalfa M30140ci (KYOCERA), 7009ci, 6009ci, 5009ci, 4009ci (TA Triumph-Adler/UTAX), with FAX System With system firmware C2G_S000.001.226 and FAX System 14
Security Target Identification	TASKalfa MZ7001ci, TASKalfa MZ6001ci, TASKalfa MZ5001ci, TASKalfa MZ4001ci Series with FAX System Security Target, 2025-12-02, version 1.02
EAL	EAL 2 + ALC_FLR.2
Sponsor	KYOCERA document solutions Inc.
Developer	KYOCERA document solutions Inc.
ITSEF	Combitech AB
Common Criteria version	CC:2022
CEM version	CEM:2022
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2026-02-26

3 Security Policy

The TOE provides the following security services:

- User Management
- Data Access Control
- FAX Data Flow Control
- SSD Encryption
- Audit Log
- Security Management
- Self-Test
- Network Protection

3.1 User Management

User Management function 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

The data access control function allows authorized users only to access to image data 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.

3.3 FAX Data Flow Control

FAX Data Flow Control function forwards the data received from public line to the TOE's external interface, following to the FAX forward setting.

3.4 SSD Encryption

SSD Encryption function encrypts information assets stored in the SSD in order to prevent leakage of data stored in the SSD inside the TOE.

3.5 Audit Log

Audit Log function records and stores the audit logs of user operations and security-relevant events on the SSD. 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.

3.6 Security Management

Security Management function 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.

3.7 Self-Test

Self-Test function verifies the integrity of TSF executable code and TSF data to detect unauthorized alteration of the executable code of the TOE security functions.

3.8 Network Protection

Network Protection function 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 an MFP is exception.

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
  The hardware and software that are composed of TOE 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

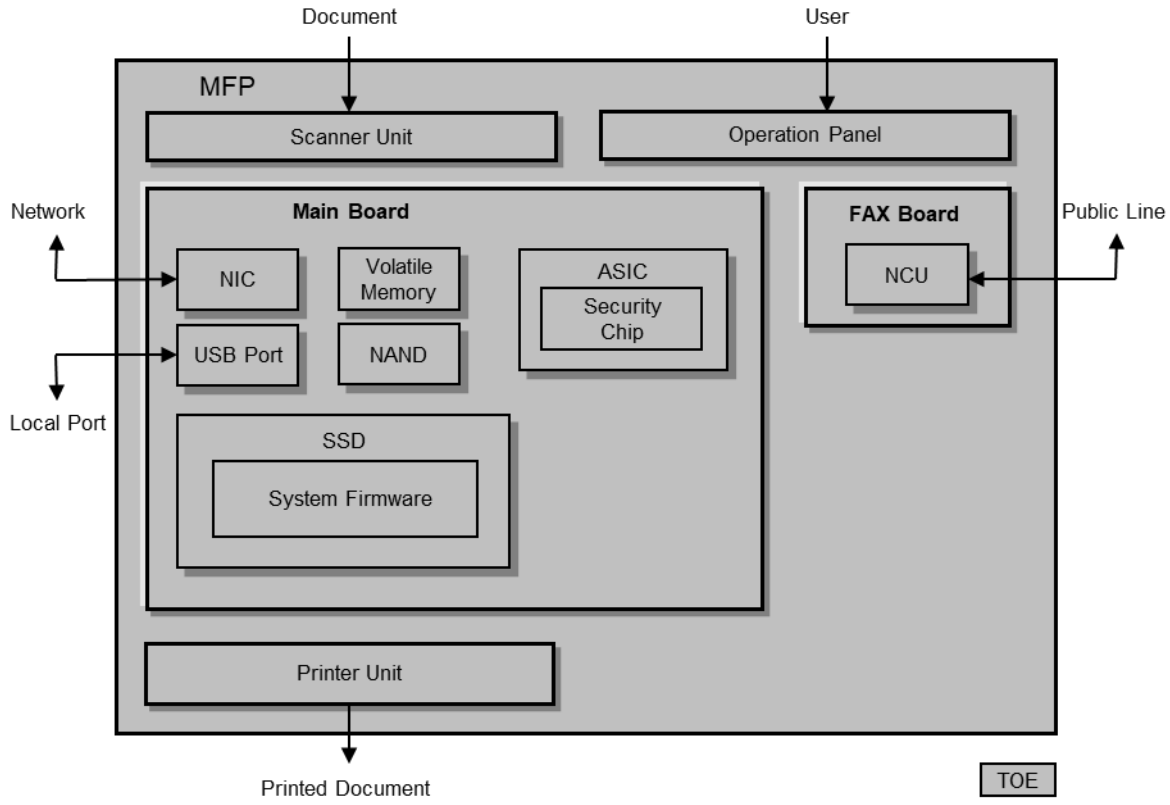
The Security Target contains three threats, which have been considered during the evaluation.

- 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 image data via the operation panel or Client PC and leak or alter them.
- T.NETWORK
  Malicious person may illegally eavesdrop or alter image 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.SSD_ENCRYPTION
  TOE must encrypt image data and TOE setting data stored on SSD.
- P.FAX_CONTROL
  TOE must control forwarding data received from public line and send it to external interface according with rules set by authorized roles.
- P.SOFTWARE_VERIFICATION
  TOE must execute Self Test that verify execution code of TSF to detect corruption of executable code.

5 Architectural Information



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

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 an SSD, which is positioned on the Main Board. The Main Board has a Network Interface (NIC) and a Local Interface (USB Port).

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 SSD encryption function.

A FAX Board has a Public Line Interface (NCU) as an interface.

As for memory mediums, a NAND that stores device settings, a Volatile Memory that is used as working area and an SSD for the system firmware installation or image data are positioned on the Main Board. Any of the above memory mediums are not removable. Image data handled by other basic functions is stored in the SSD.

6 Documentation

The following guidance documents are part of the TOE:

Document name	Version
ISO 15408 Notice (KYOCERA)	C2GIEEEKD01
ISO 15408 Notice (KYOCERA)	C2GIEEEKR01
ISO 15408 Notice (TA Triumph-Adler/UTAX)	C2GIEEEGE01
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i First Steps Quick Guide (KYOCERA)	3VC2G5601001
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Operation Guide (KYOCERA)	C2GKDEN002
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Safety Guide (KYOCERA)	3VC2G5622001
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i FAX Operation Guide	C2GKDEN501
Data Encryption/Overwrite Operation Guide	3MSC2GKDEN01
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Command Center RX User Guide	C2GCCRXKDEN32
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Printer Driver User Guide (KYOCERA)	C2GCLKTEN842
KYOCERA Net Direct Print User Guide	DirectPrintKDEN7

7 IT Product Testing

7.1 Developer Testing

All TOE variants included in the evaluation use the same firmware: C2G_S000.001.226, and execute on the same main board with the same processor.

The developer testing was performed on TASKalfa MZ4001ci, TASKalfa MZ5001ci, TASKalfa MZ6001ci, and TASKalfa MZ7001ci.

The developer divided testing into eight categories:

1. User Management Function
2. Job Authentication Function
3. Data Access Control Function
4. Encryption Overwrite Function
5. Audit Log Function
6. Security Management Function
7. Self Test Function
8. Network Protection Function

Testing was extensive and all test results were as expected.

7.2 Evaluator Testing

The evaluator testing was performed in the evaluator's premises in Bromma, Sweden, between 2025-06-18 and 2025-07-03.

All TOE variants included in the evaluation use the same firmware: C2G_S000.001.226, and execute on the same main board with the same processor.

The evaluator testing was performed on TASKalfa MZ7001ci.

The evaluator executed several developer tests, and additional new tests. All categories above except Self Test, due to lack of tooling, were covered by evaluator testing. Approximately 25% of developer tests were executed by the evaluator. All test results were as expected.

7.3 Penetration Testing

The TASKalfa MZ7001ci. model was used for penetration testing.

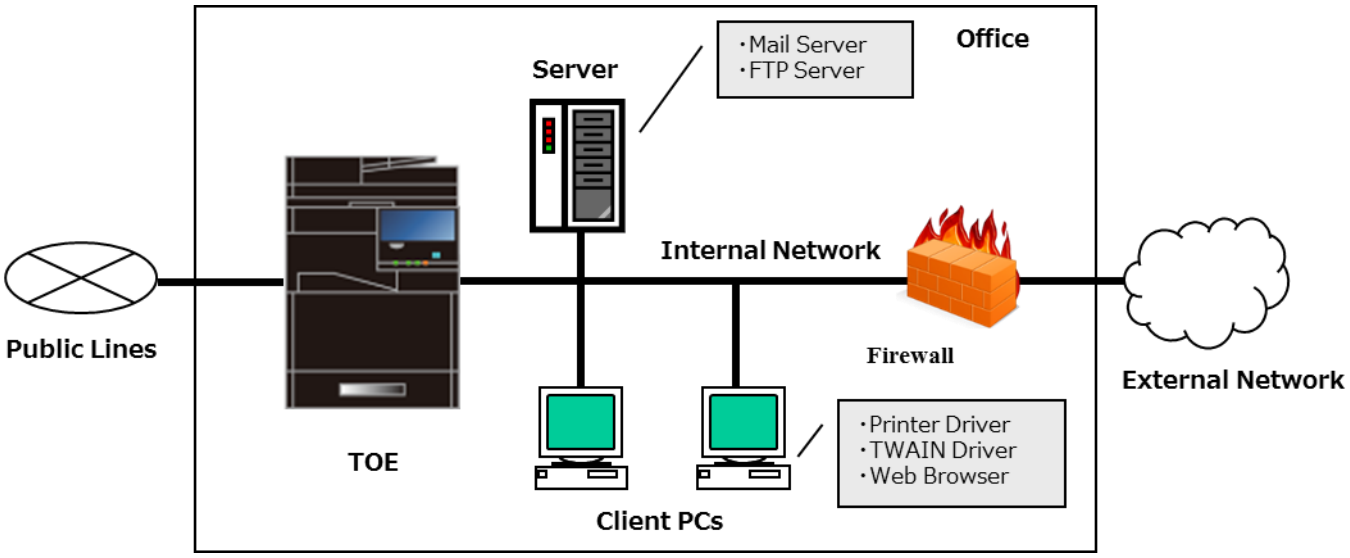
The evaluators performed port scans (NMAP), vulnerability scan (Nessus), and jpeg fuzz tests (Peach).

The testing took place in Combitech's premises in Bromma, Sweden, 2025-07-03.

No vulnerabilities were found during the penetration testing.

8 Evaluated Configuration

Normal user environment.



Required Non-TOE Hardware, Software and Firmware name is as follows.

- Client PCs:
  - Printer Driver: KX Driver
  - TWAIN Driver: Kyocera TWAIN Driver
  - Web Browser: Microsoft Edge
- Mail Server: IPsec (IKEv1) should be available.
- FTP Server: IPsec (IKEv1) should be available.

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 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
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
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
Security Target evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Extended component definition	ASE_ECD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.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
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 MZ7001ci, TASKalfa MZ6001ci, TASKalfa MZ5001ci, TASKalfa MZ4001ci Series with FAX System Security Target, KYOCERA Document Solution Inc., Combitech, 2025-12-02, document version 1.02, FMV ID 24FMV6689-47
N1	ISO 15408 Notice (KYOCERA), 2025-08, C2GIEEEKD01
N2	ISO 15408 Notice (KYOCERA), 2025-08, C2GIEEEKR01
N3	ISO 15408 Notice (TA Triumph-Adler/UTAX), 2025-08, C2GIEEEGE01
QG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i First Steps Quick Guide (KYOCERA), 2024-06, 3VC2G5601001
OG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Operation Guide (KYOCERA), 2024-11, C2GKDEN002
SG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Safety Guide (KYOCERA), 2024-06, 3VC2G5622001
FAX-OG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i FAX Operation Guide, 2025-01, C2GKDEN501
DE-OOG	Data Encryption/Overwrite Operation Guide, 2025-09, 3MSC2GKDEN01
UG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Command Center RX User Guide, 2024-12, C2GCCRXKDEN32
PD-UG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Printer Driver User Guide (KYOCERA), 2025-04, C2GCLKTEN842
DP	KYOCERA Net Direct Print User Guide, 2025-03, DirectPrintKDEN7

CC/CEM	Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, CCMB-2022-11-001 through 006, document versions CC:2022/CEM:2022 rev 1

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
2.6.1	2025-10-16	No impact
2.6	2025-04-23	No impact
2.5.2	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on the Security Target	Compliant
SN-22	4.0	Vulnerability assessment	Compliant
SN-27	1.0	ST requirements at the time of application for certification	Compliant
SN-28	2.0	Updated procedures for application, evaluation and certification	Compliant