



Swedish Certification Body for IT Security

Certification Report Kyocera TASKalfa MZ2501ci HDD

Issue: 1.0, 2026-feb-26

Authorisation: Michael Lindh Almér, Lead Certifier, CSEC

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa MZ2501ci HDD

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 Function	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	16
11	Glossary	17
12	Bibliography	18
Appendix A	Scheme Versions	20
A.1	Scheme/Quality Management System	20
A.2	Scheme Notes	20

1 Executive Summary

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

- KYOCERA TASKalfa MZ3501ci
- KYOCERA TASKalfa MZ2501ci
- KYOCERA TASKalfa M30135ci
- KYOCERA TASKalfa M30125ci
- TA Triumph-Adler 3509ci
- TA Triumph-Adler 2509ci
- UTAX 3509ci
- UTAX 2509ci

With the system firmware C2L_S000.001.226, FAX System 14 and Hard Disk Option (HD-15). However, the HDD option (HD-15) is not required in the case of the product supports HDD as standard.

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.

This Security Target claims conformance to the following Protection Profile:

- [PP2600.2]: IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hard-copy Devices, Operational Environment B", 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 Bromma, Sweden, and was completed on the February 2, 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).

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa MZ2501ci HDD

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	CSEC2024020
Name and version of the certified IT product	KYOCERA TASKalfa MZ3501ci, TASKalfa MZ2501ci, TASKalfa M30135ci, TASKalfa M30125ci (KYOCERA), 3509ci, 2509ci (TA Triumph-Adler/UTAX), with Hard Disk and FAX System With system firmware C2L_S000.001.226, FAX System 14 and Hard Disk Option (HD-15)
Security Target Identification	TASKalfa MZ3501ci, TASKalfa MZ2501ci Series with Hard Disk and FAX System Security Target, 2025-12-02, version 1.02
EAL	EAL 2 + ALC_FLR.2
PP claim	[PP2600.2]: IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hard-copy Devices, Operational Environment B", v1.0, including the PRT, SCN, CPY, FAX, DSR and SMI packages, in accordance with NIAP CCEVS Policy Letter #20.
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
- Job Authorization
- HDD Encryption
- Overwrite-Erase
- 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 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 Function

Job Authorization Function 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

HDD Encryption Function 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

Overwrite-Erase Function 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

Audit Log function 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

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.

3.8 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.

3.9 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 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

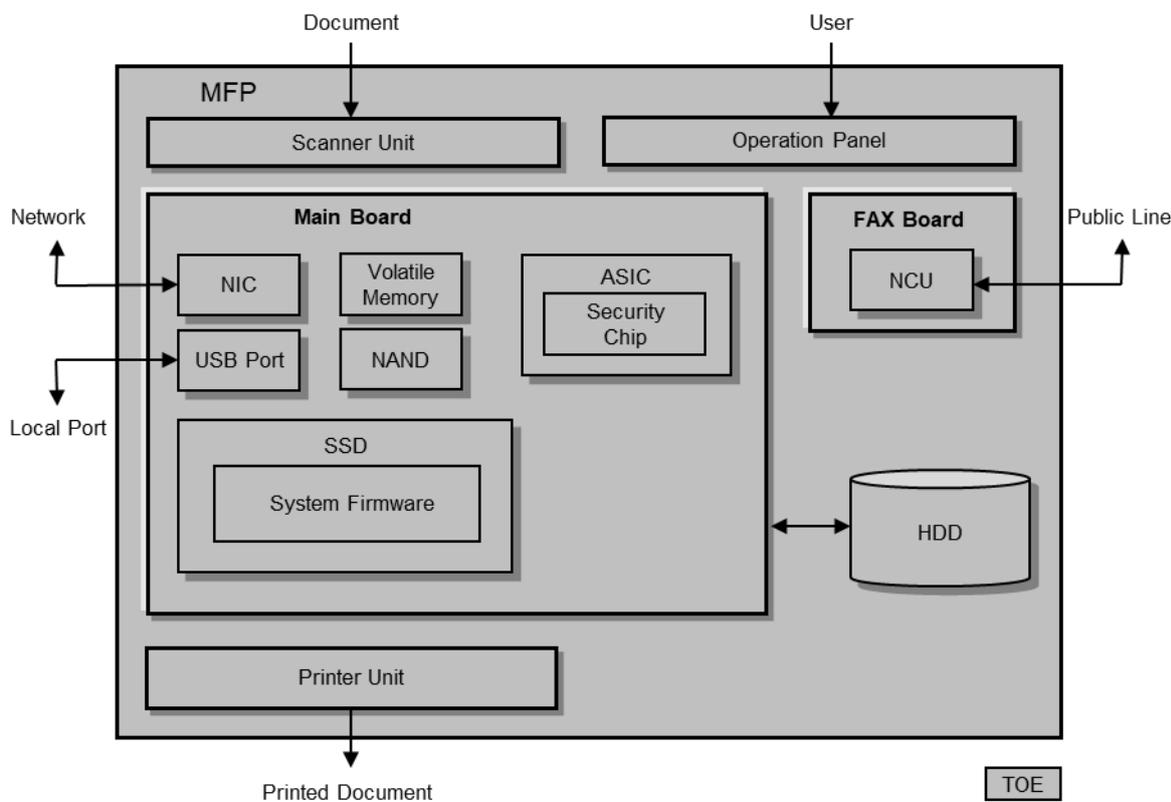
The Security Target contains five Organisational Security Policies (OSPs), which have been considered during the evaluation.

- **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.

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa MZ2501ci HDD

- **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



The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Main Board, a FAX Board, HDD and 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 HDD encryption function and HDD Overwrite-Erase 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 are positioned on the Main Board. An HDD that stores image data and job data, is connected to the Main Board. Any of the above memory mediums are not removable. Image data handled by other basic functions is stored in the HDD. However, image data is not stored in the SSD.

6 Documentation

The following guidance documents are part of the TOE:

Document name	Version
ISO 15408 Notice (KYOCERA)	C2LIEEEKD01
ISO 15408 Notice (KYOCERA)	C2LIEEEKR01
ISO 15408 Notice (TA Triumph-Adler/UTAX)	C2LIEEEGE01
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASK- alfa 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 / TASK- alfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Operation Guide (KYOCERA)	C2GKDEN002
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASK- alfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Safety Guide (KYOCERA)	3VC2G5622001
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASK- alfa 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 / TASK- alfa 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 / TASK- alfa 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: C2L_S000.001.226, and execute on the same main board with the same processor.

The developer testing was performed on MZ3501ci, TASKalfa MZ2501ci, TASKalfa M30135ci, TASKalfa M30125ci.

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 2025-07-02.

All TOE variants included in the evaluation use the same firmware: C2L_S000.001.226, and execute on the same main board with the same processor.

The evaluator testing was performed on TASKalfa MZ3501ci.

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 MZ3501ci model was used for penetration testing.

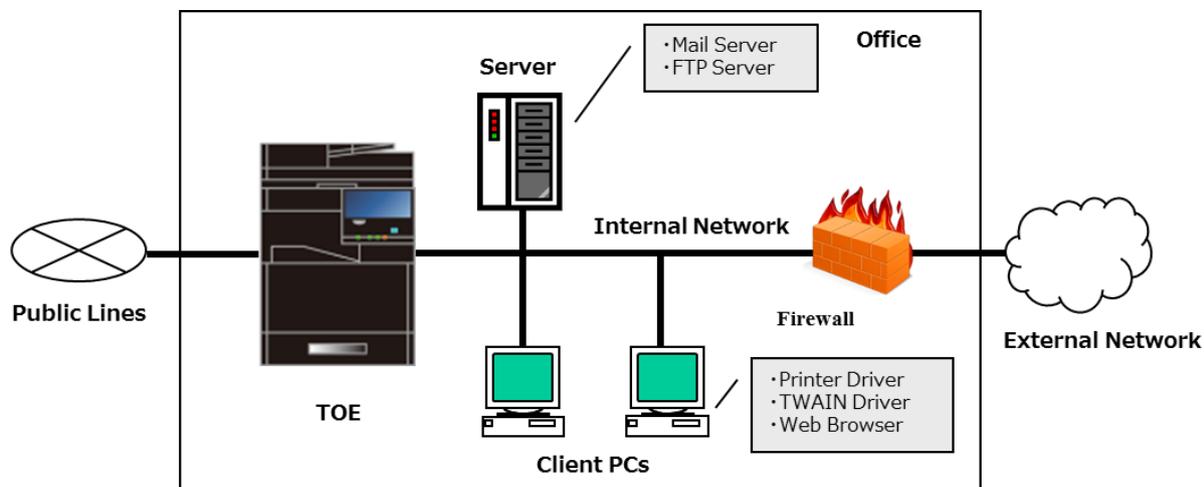
The evaluators performed port scans (NMAP), vulnerability scan (Nessus), and jpeg fuzz tests (Peach).

The testing took place in Combitech's premises in Bromma, Sweden, 2025-07-02.

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

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa MZ2501ci HDD

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 MZ3501ci, TASKalfa MZ2501ci Series with Hard Disk and FAX System, Security Target, KYOCERA Document Solution Inc., version 1.02, 2025-12-02, FMV ID 24FMV6692-37
- PP2600.2 IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hard-copy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20), version 1.0, 2009-12-09
- N1 ISO 15408 Notice (KYOCERA), 2025-08, C2LIEEEKD01
- N2 ISO 15408 Notice (KYOCERA), 2025-08, C2LIEEEKR01
- N3 ISO 15408 Notice (TA Triumph-Adler/UTAX), 2025-08, C2LIEEEGE01
- 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),

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa MZ2501ci HDD

2025-04, C2GCLKTEN842

DP	KYOCERA Net Direct Print User Guide, 2025-03, Direct-PrintKDEN7
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