



Swedish Certification Body for IT Security

Certification Report Kyocera TASKalfa VFM351ci

Issue: 1.0, 2024-maj-02

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa VFM351ci

Table of Contents

1	Executive Summary	3
2	Identification	4
3	Security Policy	5
3.1	User Management	5
3.2	Data Access Control	5
3.3	FAX Data Flow Control	5
3.4	SSD Encryption	5
3.5	Audit Log	5
3.6	Security Management	5
3.7	Self-Test	6
3.8	Network Protection	6
4	Assumptions and Clarification of Scope	7
4.1	Assumptions	7
4.2	Clarification of Scope	7
5	Architectural Information	8
6	Documentation	9
7	IT Product Testing	10
7.1	Developer Testing	10
7.2	Evaluator Testing	10
7.3	Penetration Testing	10
8	Evaluated Configuration	11
9	Results of the Evaluation	12
10	Evaluator Comments and Recommendations	13
11	Glossary	14
12	Bibliography	15
Appendix A	Scheme Versions	17
A.1	Scheme/Quality Management System	17
A.2	Scheme Notes	17

1 Executive Summary

The TOE is the hardware and the firmware of the following Multifunction Printer (MFP) models with FAX:

KYOCERA: TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 3554ciG, TASKalfa 2554ciG, TASKalfa VFM351ci, TASKalfa VFM251ci, TA Triumph-Adler: 3508ci, 2508ci, and UTAX: 3508ci, 2508ci.

All models have the system firmware:

2XD_S0IS.C03.317,

and the FAX firmware:

3R2_5100.003.012.

In the evaluated configuration, the FAX System 12 shall be installed.

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

Delivery is done by means of a courier trusted by KYOCERA Document Solutions Inc. with pre-installed firmware and guidance documentation. The FAX board is delivered separately.

No PP is claimed.

The evaluation has been performed by Combitech in their premises in Bromma and Växjö, Sweden. The evaluation was completed on the eleventh of April 2024.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC) 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	CSEC2023008
Name and version of the certified IT product	KYOCERA: TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 3554ciG, TASKalfa 2554ciG, TASKalfa VFM351ci, TASKalfa VFM251ci, TA Triumph-Adler: 3508ci, 2508ci, UTAX: 3508ci, 2508ci, all with FAX System 12 and: System firmware: 2XD_S0IS.C03.317 FAX firmware: 3R2_5100.003.012
Security Target Identification	TASKalfa 3554ci, TASKalfa 2554ci Series with FAX System Security Target, v1.20
EAL	EAL 2 + ALC_FLR.2
Sponsor	Kyocera Document Solutions Inc.
Developer	Kyocera Document Solutions Inc.
ITSEF	Combitech AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.5.1
Scheme Notes Release	21.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2024-05-02

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

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 so that only authorized users can access to image data stored in the TOE.

3.3 FAX Data Flow Control

A function that controls forwarding the data received from public line to the TOE's external interface, following to the FAX forward setting.

3.4 SSD Encryption

A function that 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

A function that 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

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.

3.7 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.

3.8 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.

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

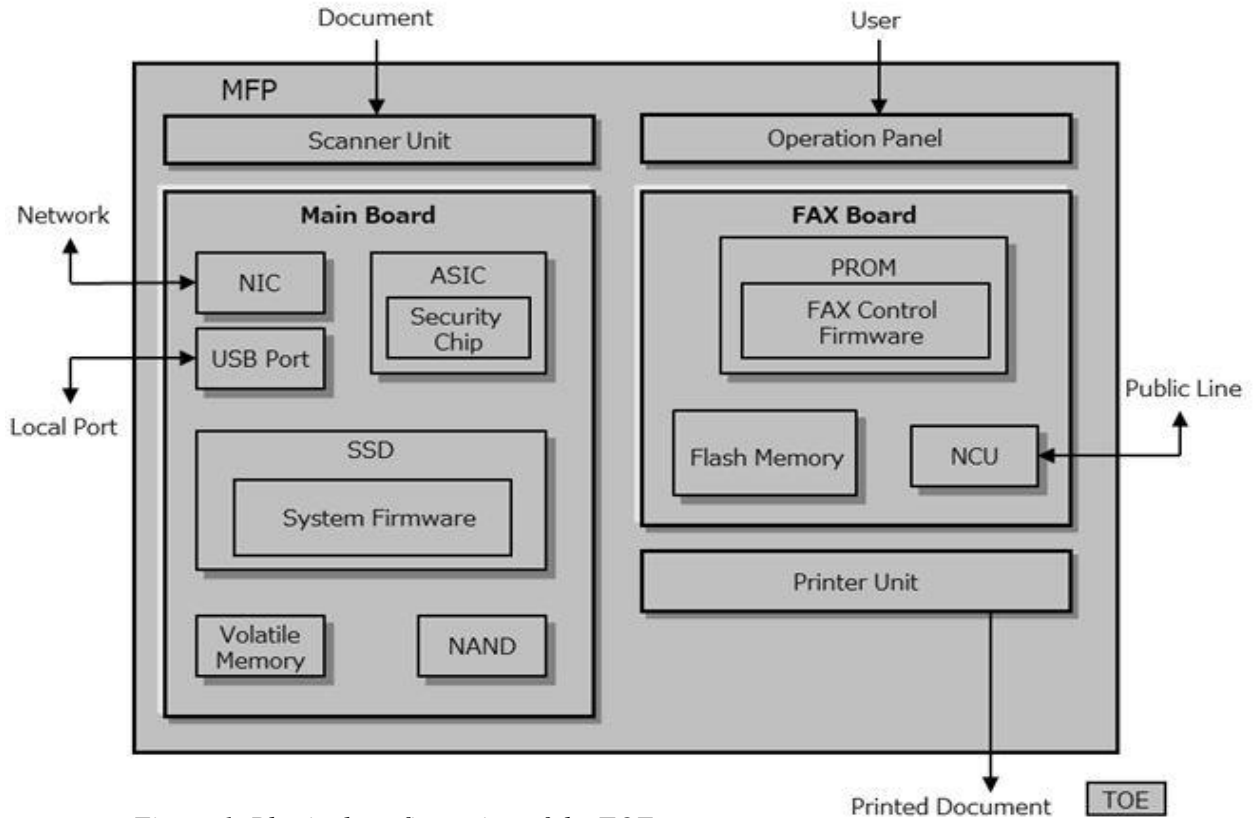


Figure 1. Physical configuration of the TOE

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

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.

6 Documentation

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

Notice (KYOCERA)

Notice (KYOCERA VFM)

Notice (Copystar)

Notice (TA Triumph-Adler/UTAX)

FAX System 12 Installation Guide

TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa VFM601ci / TASKalfa 5054ci /
TASKalfa VFM501ci / TASKalfa 4054ci / TASKalfa VFM401ci / TASKalfa 3554ci /
TASKalfa VFM351ci / TASKalfa 2554ci / TASKalfa VFM251ci First Steps Quick
Guide

TASKalfa 2554ci / TASKalfa 3554ci / TASKalfa 4054ci / TASKalfa 5054ci / TASK-
alfa 6054ci / TASKalfa 7054ci Operation Guide

TASKalfa 2554ci / TASKalfa VFM251ci / TASKalfa 3554ci / TASKalfa VFM351ci /
TASKalfa 4054ci / TASKalfa VFM401ci / TASKalfa 5054ci / TASKalfa VFM501ci /
TASKalfa 5004i / TASKalfa VFM501i / TASKalfa 6054ci / TASKalfa VFM601ci /
TASKalfa6004i / TASKalfa VFM601i / TASKalfa 7054ci / TASKalfa 7004i Safety
Guide

FAX System 12 Operation Guide

Data Encryption/Overwrite Operation Guide

Command Center RX User Guide

TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa 5054ci / TASKalfa 4054ci / TASK-
alfa 3554ci / TASKalfa 2554ci 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 VFM251ci and the TASKalfa VFM351ci models, with system firmware 2XD_S0IS.C03.317 and FAX firmware 3R2_5100.003.012.

Each of the other models are electronically and mechanically 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 Bromma, Sweden, between 2023-12-11 and 2023-12-20. The TASKalfa 3554ci model with system firmware 2XD_S0IS.C03.317 and FAX firmware 3R2_5100.003.012 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 Bromma, Sweden, between 2023-12-11 and 2023-12-20. The TASKalfa 3554ci model with system firmware 2XD_S0IS.C03.317 and FAX firmware 3R2_5100.003.012 was used.

NMAP was used to perform a series of port scans, NESSUS was used for a vulnerability scan, 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 operational environment of the TOE, the following non-TOE hardware and software is expected:

- Client PC with a KX printer driver, a Kyocera TWAIN driver, and a Microsoft Internet Explorer 11.0 web browser
- Mail server connected via IPSec with IKE1
- FTP server connected via IPSec with IKE1

In the evaluated configuration:

- the internal network where the TOE is placed is protected by a firewall
- maintenance interfaces shall not be available

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

CC	Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CR	Change Request
CSEC	The Swedish CC Certification Body
FER	Final Evaluation Report
SAR	Security Assurance Requirements
SER	Single Evaluation Report
SFR	Security Functional Requirements
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

- ST TASKalfa 3554ci, TASKalfa 2554ci Series with FAX System Security Target, Kyocera Document Solutions Inc., 2023-12-27, document version 1.20, FMV ID 23FMV3866-13
- Notice1 Notice (KYOCERA), Kyocera Document Solutions Inc., 2023-12, document version 302XD5641003, FMV ID 23FMV3866-13
- Notice2 Notice (KYOCERA VFM), Kyocera Document Solutions Inc., 2023-12, document version 302XD5644001, FMV ID 23FMV3866-13
- Notice3 Notice (Copystar), Kyocera Document Solutions Inc., 2020-09, document version 302XD5642001, FMV ID 23FMV3866-13
- Notice4 Notice (TA Triumph-Adler/UTAX), Kyocera Document Solutions Inc., 2023-12, document version, 302XD5643003, FMV ID 23FMV3866-13
- FAXIG FAX System 12 Installation Guide, Kyocera Document Solutions Inc., 2019-08, document version 303RK5671101, FMV ID 23FMV3866-13
- QG TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa VFM601ci / TASKalfa 5054ci / TASKalfa VFM501ci / TASKalfa 4054ci / TASKalfa VFM401ci / TASKalfa 3554ci / TASKalfa VFM351ci / TASKalfa 2554ci / TASKalfa VFM251ci First Steps Quick Guide, Kyocera Document Solutions Inc., 2022-05, document version 302XC5606002, FMV ID 23FMV3866-13
- OG TASKalfa 2554ci / TASKalfa 3554ci / TASKalfa 4054ci / TASKalfa 5054ci / TASKalfa 6054ci / TASKalfa 7054ci Operation Guide, Kyocera Document Solutions Inc., 2020-09, document version 2XCKDEN000, FMV ID 23FMV3866-13
- SG TASKalfa 2554ci / TASKalfa VFM251ci / TASKalfa 3554ci / TASKalfa VFM351ci / TASKalfa 4054ci / TASKalfa VFM401ci / TASKalfa 5054ci / TASKalfa VFM501ci / TASKalfa 5004i / TASKalfa VFM501i / TASKalfa 6054ci / TASKalfa VFM601ci / TASKalfa6004i / TASKalfa VFM601i / TASKalfa 7054ci / TASKalfa

Swedish Certification Body for IT Security
Certification Report Kyocera TASKalfa VFM351ci

7004i Safety Guide, Kyocera Document Solutions Inc., 2022-02,
document version 302XC5628001, FMV ID 23FMV3866-13

FAXOG	FAX System 12 Operation Guide, Kyocera Document Solutions Inc., 2020-02, document version 3RKKDEN300, FMV ID 23FMV3866-13
DE	Data Encryption/Overwrite Operation Guide, Kyocera Document Solutions Inc., 2020-09, document version 3MS2XCCKDEN1, FMV ID 23FMV3866-13
CCRX	Command Center RX User Guide, Kyocera Document Solutions Inc., 2020-02, document version CCRXKDEN23, FMV ID 23FMV3866-13
PD	TASKalfa 7054ci / TASKalfa 6054ci / TASKalfa 5054ci / TASKalfa 4054ci / TASKalfa 3554ci / TASKalfa 2554ci Printer Driver User Guide, Kyocera Document Solutions Inc., 2020-02, document version 2XCCLKTEN750.2020.02, FMV ID 23FMV3866-13
NDP	KYOCERA Net Direct Print User Guide, Kyocera Document Solutions Inc., 2019-02, document version DirectPrintKDEN2.2019.2, FMV ID 23FMV3866-13
EP-002	002 Evaluation and Certification, CSEC, 2023-Jun-02, document version 35.0
CC3.1	Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, CCMB-2017-04, 001 through 004, document version 3.1 revision 5

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
2.5.1	2024-02-29	None
2.5	2024-01-25	None
2.4.1	2023-09-14	None
2.4	Application	Original version

A.2 Scheme Notes

Scheme Notes applicable to the certification

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	3.0	Highlighted Requirements on the ST	Compliant
SN-22	4.0	Vulnerability Assessment	Compliant
SN-27	1.0	ST Requirement at the Time of Application	Compliant
SN-28	2.0	Updated Procedures	Compliant