



Swedish Certification Body for IT Security

Certification Report - Kyocera TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk and FAX System

Issue: 1.0, 2021-May-12

Authorisation: Helén Svensson, Lead Certifier , CSEC



Ärendetyp: 6

Diarienummer: 20FMV3464-31:1

Dokument ID

Swedish Certification Body for IT Security
Certification Report - Kyocera TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk
and FAX System

Table of Contents

1	Executive Summary	3
2	Identification	5
3	Security Policy	6
3.1	User Management Function	6
3.2	Data Access Control Function	6
3.3	Job Authorization Function	6
3.4	HDD Encryption Function	7
3.5	Overwrite-Erase Function	7
3.6	Audit Log Function	7
3.7	Security Management Function	7
3.8	Self-Test Function	7
3.9	Network Protection Function	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	18
A.1	Scheme/Quality Management System	18
A.2	Scheme Notes	18

1 Executive Summary

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

- KYOCERA TASKalfa 3554ci, KYOCERA TASKalfa 2554ci, KYOCERA TASKalfa 3554ciG, KYOCERA TASKalfa 2554ciG,
- Copystar CS 3554ci, Copystar CS 2554ci,
- TA Triumph-Adler 3508ci, TA Triumph-Adler 2508ci,
- UTAX 3508ci, UTAX 2508ci

with the following firmware:

System Firmware: 2XD_S000.002.206

FAX Firmware: 3R2_5100.003.012

and the following additional options:

- Hard Disk Option (HD-15)
- FAX Option (FAX System 12)

The HDD option (HD-15) is not required in the case of the product supports HDD as standard, for more information see [ST] Table 1-2

The TOE provides Copy function, Scan function, Print function, FAX function and Box function.

Information about the delivery method for each TOE components can be found in [ST] Table 1-3.

The TOEs claim demonstrable conformance to IEEE Std 2600.2-2009; “2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B” (with NIAP CCEVS Policy Letter #20) ([PP2600.2]), version 1.0.

The evaluation has been performed by Combitech AB in Växjö and Bromma.

The evaluation was completed on 2021-04-14. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 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. (Repeat if more than one ITSEF is involved)

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.

Swedish Certification Body for IT Security
Certification Report - Kyocera TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk
and FAX System

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	CSEC2020008
Name and version of the certified IT product	KYOCERA TASKalfa 3554ci, KYOCERA TASKalfa 2554ci, KYOCERA TASKalfa 3554ciG, KYOCERA TASKalfa 2554ciG, Copystar CS 3554ci, Copystar CS 2554ci, TA Triumph-Adler 3508ci, TA Triumph-Adler 2508ci, UTAX 3508ci, UTAX 2508ci with hard disk and FAX. System Firmware: 2XD_S000.002.206 FAX Firmware: 3R2_5100.003.012
Security Target Identification	TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk and FAX System, Security Target, 1.0, March 4, 2021
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	1.24.1
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2021-05-12

3 Security Policy

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

3.1 User Management Function

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 Function

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 Function

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 Function

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 Function

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 Function

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 Function

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 Function

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 Function

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

Swedish Certification Body for IT Security
Certification Report - Kyocera TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk
and FAX System

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

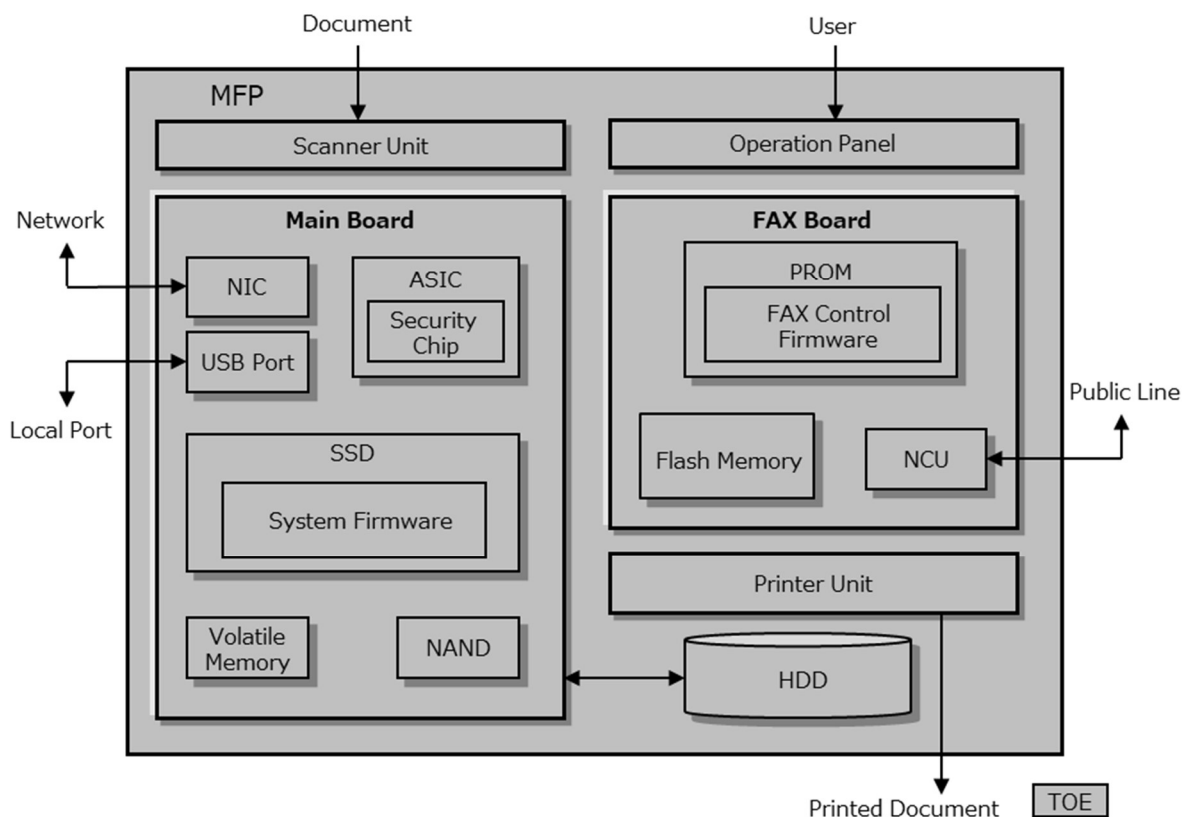


Figure 1 Physical Configuration of TOE

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Main Board, a FAX Board, HDD and SSD hardware, and 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 (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 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 documents are included in the scope of the TOE:

- Notice (KYOCERA)
- Notice (Copystar)
- Notice (TA Triumph-Adler/UTAX)
- FAX System 12 Installation Guide
- TASKalfa 3554ci / TASKalfa 2554ci First Steps Quick Guide
- TASKalfa 2554ci / TASKalfa 3554ci / TASKalfa 4054ci / TASKalfa 5054ci / TASKalfa 6054ci / TASKalfa 7054ci Operation Guide
- TASKalfa 2554ci / TASKalfa 3554ci 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 / TASKalfa 3554ci / TASKalfa 2554ci Printer Driver User Guide
- KYOCERA Net Direct Print User Guide

7 IT Product Testing

7.1 Developer Testing

The developer was executed on TASKalfa 3554ci HDD with the following firmware versions:

- System: 2_XD_S000.002.206
- FAX: 3R2_5100.003.012

The TASKalfa 3554ci and TASKalfa 2554ci series execute on the same main board with the same CPU. They all running the same set of firmwares.

The developer tests included in the CC testing cover full coverage for the TOE interfaces and most of the security functionality

7.2 Evaluator Testing

The independent testing was performed on TASKalfa 3554ci with HDD.

The TASKalfa 3554ci and TASKalfa 2554ci series execute on the same main board with the same CPU. They all running the same set of firmwares.

The evaluator performed approximately 25% of the developer tests. Some of the test cases were complemented with independent testing.

Some tools for fuzzing – PeachFuzz, port scanning – nmap, and vulnerability scanning – Nessus, were used.

The actual results of all test cases were consistent with the expected test results and all tests were judged to pass

7.3 Penetration Testing

The following types of penetration tests were performed:

- Port scan
- Vulnerability scan including web application vulnerability scan
- JPG fuzzing

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

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 Internet Explorer 11.0
- 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:

<i>Assurance Class/Family</i>	<i>Component</i>	<i>Verdict</i>
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE 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
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.2	PASS
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
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	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
EAL	Evaluation Assurance Level
FAX	facsimile
HDD	Hard Disk Drive
ITSEF	IT Security Evaluation Facility
IT	information technology
MFP	Multi Functional Printer
NCU	Network Control Unit
OSP	organizational security policy
PP	Protection Profile
SSD	Solid State Drive
ST	Security target
TOE	Target of Evaluation
TSF	TOE security functionality
USB	Universal Serial Bus

12 Bibliography

ST	TASKalfa 3554ci, TASKalfa 2554ci Series with Hard Disk and FAX System, Security Target, document version 1.0, March 4, 2021
PP2600.2	2600:2, Protection Profile for Hardcopy Devices, Operational Environment B, document version 1.0, January 2009
QG-1	First Steps Quick Guide TASKalfa 3554ci, TASKalfa 2554ci, Kyocera Document Solutions Inc., document version 302XC5602001, 2020.9
IG-FAX	INSTALLATION GUIDE, FAX System 12, Kyocera Document Solutions Inc., document version 303RK5671101, 2019.8
SG-1	TASKalfa 2554ci / TASKalfa 3554ci Safety Guide, Kyocera Document Solutions Inc., document version 302XC5622001, 2020.9
OG-1	OPERATION GUIDE, TASKalfa 2554ci, TASKalfa 3554ci, TASKalfa 4054ci, TASKalfa 5054ci, TASKalfa 6054c, TASKalfa 7054ci, Kyocera Document Solutions Inc., document version 2XCKDEN000, 2020.9
OG-FAX	FAX System 12 Operation Guide, Kyocera Document Solutions Inc., document version 2RKKDEN300, 2020.2
DE-1	Data Encryption/Overwrite, Operation Guide, Kyocera Document Solutions Inc., document version 3MS2XCKDEN1, 2020.9
PD-1	Printer Driver, User Guide, TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci, TASKalfa 3554ci, TASKalfa 2554c, Kyocera Document Solutions Inc., document version 2XCCLKTEN750, 2020.2
CCRX-1	User Guide, Command Center RX, Kyocera Document Solutions Inc., document version CCRXKDEN23, 2020.2
NDP	KYOCERA Net Direct Print User Guide, Kyocera Document Solutions Inc., document version DirectPrintKDEN2, 2019.2
NOTICE-1	Notice (TA Triumph-Adler/UTAX), Kyocera Document Solutions Inc., document version 302XD5643001, 2020.9
NOTICE-2	Notice (Copystar), Kyocera Document Solutions Inc., document version 302XD5642001, 2020.9
NOTICE-3	Notice (KYOCERA), Kyocera Document Solutions Inc., document version 302XD5641001, 2020.9
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2020-11-30, document version 32.0

Appendix A **Scheme Versions**

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

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.23.2 valid from 2020-05-11

QMS 1.24 valid from 2020-11-19

QMS 1.24.1 valid from 2020-12-03

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 1.24.1”. The certifier concluded that, from QMS 1.23.2 to the current QMS 1.24.1, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 28 - Updated procedures for application, evaluation and certification