**Swedish Certification Body for IT Security**

# Certification Report Kyocera MA4000

**Issue: 1.0, 2023-sep-14**

*Authorisation: Jerry Johansson, Lead certifier , CSEC*

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 FAX Data Flow Control 6
3.4 SSD Encryption 6
3.5 Security Management 6
3.6 Network Protection 6

**4 Assumptions and Clarification of Scope 7**
4.1 Usage 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 SSD:

Kyocera
ECOSYS MA4000cifx/cifxG,
ECOSYS MA3500cifx/cifxG,
TASKalfa MA4500ci,
TASKalfa MA3500ci,
Copystar CS MA4500ci,
TA Triumph-Adler
P-C4067i MFP,
P-C3567i MFP,
458ci,
358ci,
UTAX
P-C4067i MFP,
P-C3567i MFP,
458ci, or
358ci.

with system firmware

2Z7_S0IS.C03.002

In the evaluated configuration, the solid state drive HD-18 (SSD) is installed and is included in the scope of the TOE.

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 SSD is delivered separately.

No PP is claimed.

The evaluation has been performed by Combitech in their premises in Bromma, Sweden.

The evaluation was completed on the 25th of August 2023.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 revision 5, and Common Evaluation Methodology (CEM), 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.

# 2 Identification

| Certification Identification | |
|---|---|
| Certification ID | CSEC2021010 |
| Name and version of the certified IT product | KYOCERA ECOSYS MA4000cifx,<br>KYOCERA ECOSYS MA3500cifx,<br>KYOCERA ECOSYS MA4000cifxG,<br>KYOCERA ECOSYS MA3500cifxG,<br>KYOCERA TASKalfa MA4500ci,<br>KYOCERA TASKalfa MA3500ci,<br>Copystar CS MA4500ci,<br>TA Triumph-Adler P-C4067i MFP,<br>TA Triumph-Adler P-C3567i MFP,<br>TA Triumph-Adler 458ci,<br>TA Triumph-Adler 358ci,<br>UTAX P-C4067i MFP,<br>UTAX P-C3567i MFP,<br>UTAX 458ci,<br>UTAX 358ci<br>all with SSD and with system firmware 2Z7_S0IS.C03.002 |
| Security Target Identification | ECOSYS MA4000cifx, ECOSYS MA3500cifx, TASKalfa MA4500ci, TASKalfa MA3500ci Series with SSD Security Target |
| 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 | 2.4 |
| Scheme Notes Release | 20.0 |
| Recognition Scope | CCRA, SOGIS, EA/MLA |
| Certification date | 2023-09-14 |

# 3 Security Policy

The TOE provides the following securite services:

- User Management
- Data Access Control
- FAX Data Flow Control
- SSD Encryption
- Security Management
- 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 Box document data stored in the TOE.

## 3.3 FAX Data Flow Control

A function that controls not to forward the data received from a public line to the internal network that the TOE is connected.

## 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 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.

## 3.6 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 Usage Assumptions

The Security Target [ST] makes four assumptions on the usage and on the operational environment of the TOE.

A.ACCESS

The hardware and software that the TOE is composed of 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 box document data via the operation panel or Client PC and leak or alter them.

T.NETWORK

Malicious person may illegally eavesdrop or alter document data or TOE setting data on the internal network.

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

P.SSD_ENCRYPTION

TOE must encrypt document data and TOE setting data stored on SSD.

P.FAX_CONTROL

TOE must control not to forward the data received from a public line to the internal network that the TOE is connected.

# 5 Architectural Information

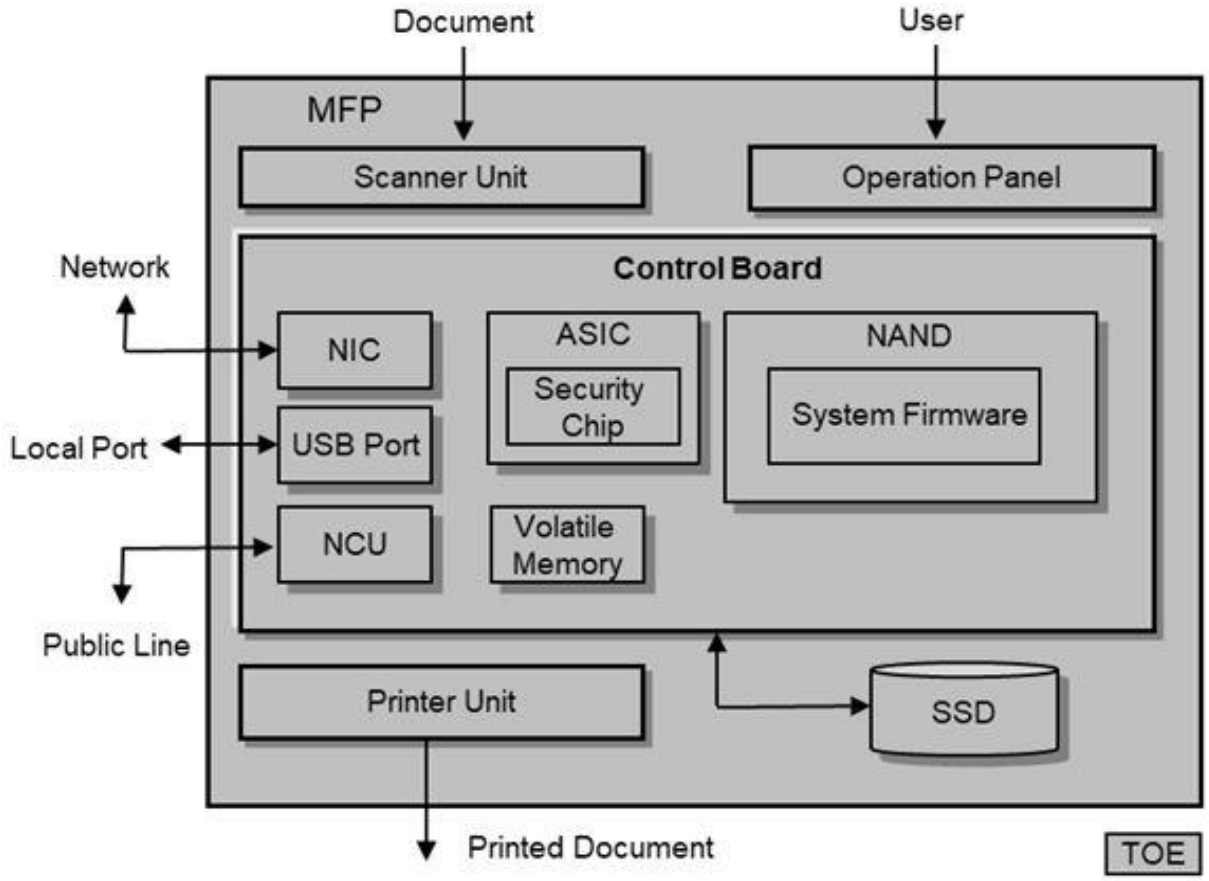


*Figure 1. Physical configuration of the TOE*

The TOE consists of an Operation Panel, a Scanner Unit, a Printer Unit, a Control Board, a SSD hardware, and a 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 Control Board is the circuit board to control entire TOE. A system firmware is installed on a NAND, which is positioned on the Control Board. The Control Board has a Network Interface (NIC), a Local Interface (USB Port), and a Public Line Interface (NCU) for the FAX functionality.

An ASIC that is also on the Control Board includes a Security Chip, which implements several security functions, such as arithmetic processing for the SSD encryption function.

# 6 Documentation

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

Notice (KYOCERA, Copystar)

Notice (TA Triumph-Adler/UTAX)

ECOSYS MA4000cifx, ECOSYS MA4000cix, ECOSYS MA3500cifx, ECOSYS MA3500cix Setup Guide

TASKalfa MA4500ci, TASKalfa MA3500ci Operation Guide

ECOSYS MA4000cifx, ECOSYS MA4000cix, ECOSYS MA3500cifx, ECOSYS MA3500cix Operation Guide

TASKalfa MA4500ci, TASKalfa MA3500ci Safety Guide

ECOSYS MA4000cifx, ECOSYS MA4000cix, ECOSYS MA3500cifx, ECOSYS MA3500cix Safety Guide

TASKalfa MA4500ci, TASKalfa MA3500ci FAX Operation Guide

ECOSYS MA4000cifx, ECOSYS MA3500cifx FAX Operation Guide

Data Encryption/Overwrite Operation Guide

Command Center RX User Guide

ECOSYS MA4000cifx, ECOSYS MA3500cifx, ECOSYS MA4000cix, ECOSYS MA3500cix, ECOSYS PA4500cx, ECOSYS PA4000cx, ECOSYS PA3500cx, TASKalfa MA4500ci, TASKalfa MA3500ci, TASKalfa PA4500ci 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 MA4500ci, and TASKalfa MA3500ci models, with system firmware 2Z7_S0IS.C03.002.

Each of the other models are functionally 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 2022-02-09 and 2023-04-13. The MA4500ci model with system firmware 2Z7_S0IS.C03.002 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 2022-02-09 and 2023-04-13. The MA4500ci model with system firmware 2Z7_S0IS.C03.002 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, and TestSSLServer was used for verifying the selection of TLS cipher suites. The evaluators verified, by testing, that CVE-2022-1026 is not exploitable for the TOE. 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 Edge web browser
- Mail server connected via IPSec with IKE1
- FTP server connected via IPSec with IKE1

In the evaluated configuration:

- a solid state disk drive (SSD) HD-18 shall be installed and is included in the scope of the TOE
- 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 | ECOSYS MA4000cifx, ECOSYS MA3500cifx, TASKalfa MA4500ci, TASKalfa MA3500ci Series with SSD Security Target, Kyocera Document Solutions Inc., 2023-04-17, document version 1.02, FMV ID 21FMV6803-14 |
| Notice1 | Notice (KYOCERA, Copystar), Kyocera Document Solutions Inc., 2023-04, document version 3V2Z55650001, FMV ID 21FMV6803-14 |
| Notice2 | Notice (TA Triumph-Adler/UTAX), Kyocera Document Solutions Inc., 2023-04, document version 3V2Z55651001, FMV ID 21FMV6803-14 |
| SG | ECOSYS MA4000cifx, ECOSYS MA4000cix, ECOSYS MA3500cifx, ECOSYS MA3500cix Setup Guide, Kyocera Document Solutions Inc., 2022-02, document version 302Z55620001, FMV ID 21FMV6803-14 |
| OG-TAS | TASKalfa MA4500ci, TASKalfa MA3500ci Operation Guide, Kyocera Document Solutions Inc., 2022-02, document version 2Z7KDEN000, FMV ID 21FMV6803-14 |
| OG-ECO | ECOSYS MA4000cifx, ECOSYS MA4000cix, ECOSYS MA3500cifx, ECOSYS MA3500cix Operation Guide, Kyocera Document Solutions Inc., 2022-02, document version 2Z5KDEN000, FMV ID 21FMV6803-14 |
| SG-TAS | TASKalfa MA4500ci, TASKalfa MA3500ci Safety Guide, Kyocera Document Solutions Inc., 2022-02, document version 3V25621001, FMV ID 21FMV6803-14 |
| SG-ECO | ECOSYS MA4000cifx, ECOSYS MA4000cix, ECOSYS MA3500cifx, ECOSYS MA3500cix Safety Guide, Kyocera Document Solutions Inc., 2022-02, document version 3V2Z55621001, |

| | |
|---|---|
| | FMV ID 21FMV6803-14 |
| FAX-TAS | TASKalfa MA4500ci, TASKalfa MA3500ci FAX Operation Guide, Kyocera Document Solutions Inc., 2022-02, document version 2Z7KDEN500, FMV ID 21FMV6803-14 |
| FAX-ECO | ECOSYS MA4000cifx, ECOSYS MA3500cifx FAX Operation Guide, Kyocera Document Solutions Inc., 2022-02, document version 3RKKDEN303, FMV ID 21FMV6803-14 |
| DEO | Data Encryption/Overwrite Operation Guide, Kyocera Document Solutions Inc., 2022-02, document version 3MS2Z7KDEN0, FMV ID 21FMV6803-14 |
| CCRX | Command Center RX User Guide, Kyocera Document Solutions Inc., 2022-02, document version CCRXKDEN25, FMV ID 21FMV6803-14 |
| PD | ECOSYS MA4000cifx, ECOSYS MA3500cifx, ECOSYS MA4000cix, ECOSYS MA3500cix, ECOSYS PA4500cx, ECOSYS PA4000cx, ECOSYS PA3500cx, TASKalfa MA4500ci, TASKalfa MA3500ci, TASKalfa PA4500ci Printer Driver User Guide, Kyocera Document Solutions Inc., 2022-02, document version 02Z7CLKTEN820.202, FMV ID 21FMV6803-14 |
| NDP | KYOCERA Net Direct Print User Guide, Kyocera Document Solutions Inc., 2019-02, document version DirectPrintKDEN2.2019.2, FMV ID 21FMV6803-14 |
| EP-002 | 002 Evaluation and Certification, CSEC. 2023-Jun-02, document version 35.0 |
| CC 3.1 | 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 |
|---|---|---|
| 2.4 | 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 | None |
| 2.1 | 2022-01-18 | None |
| 2.0 | 2021-11-24 | None |
| 1.25 | Application | Original version |

## A.2 Scheme Notes

| Scheme Note | Version | Title | Applicability |
|---|---|---|---|
| SN-15 | 5.0 | Testing | Compliant |
| SN-18 | 3.0 | ST Requirements | Compliant |
| SN-22 | 4.0 | Vulnerability Assessment | Compliant |
| SN-27 | 1.0 | Application | Compliant |
| SN-28 | 1.0 | Updated procedures | Compliant |