Ärendetyp: 6 Diarienummer: 22FMV6373-24

Dokument ID CSEC2022012

Swedish Certification Body for IT Security

Certification Report - Kyocera ECOSYS PA6000x, PA5500x, PA5000x, PA4500x

Issue: 1.0, 2023-jun-22

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the hardware and the firmware of the following Single-Function Printer (SFP) models with SSD:

KYOCERA ECOSYS PA6000x, PA5500x, PA5000x, PA4500x, P40050x, P40045x,

TA Triumph Adler P-6034DN, P-5534DN, P-5034DN, P-4534DN,

UTAX P-6034DN, P-5534DN, P-5034DN, P-4534DN,

with system firmware

C0T_S0IS.C04.002

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 printing 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, and to some extent in the developer's premises in Osaka, Japan.

The evaluation was completed on the 2nd of June 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.

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	CSEC2022012
Name and version of the certified IT product	ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x, ECOSYS P40050x, ECOSYS P40045x (KYOCERA) P-6034DN, P-5534DN, P-5034DN, P-4534DN (TA Triumph Ader/UTAX) all with SSD and with system firmware C0T_S0IS.C04.002
Security Target Identification	ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x 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	QMS 2.4
Scheme Notes Release	20.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2023-06-22

3 Security Policy

The TOE provides the following security services:

- User Management
- Data Access 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. For Normal User, use external authentication using an external user authentication server to perform identity authentication. For Device Administrator, use external or internal authentication to perform identity authentication. Also internal authentication 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 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 Box document data stored in the TOE.

3.3 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.

3.4 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.

3.5 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 Print Function, 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 Printer 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 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 one Organisational Security Policy (OSP), which has been considered during the evaluation.

P.SSD_ENCRYPTION

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

5 Architectural Information

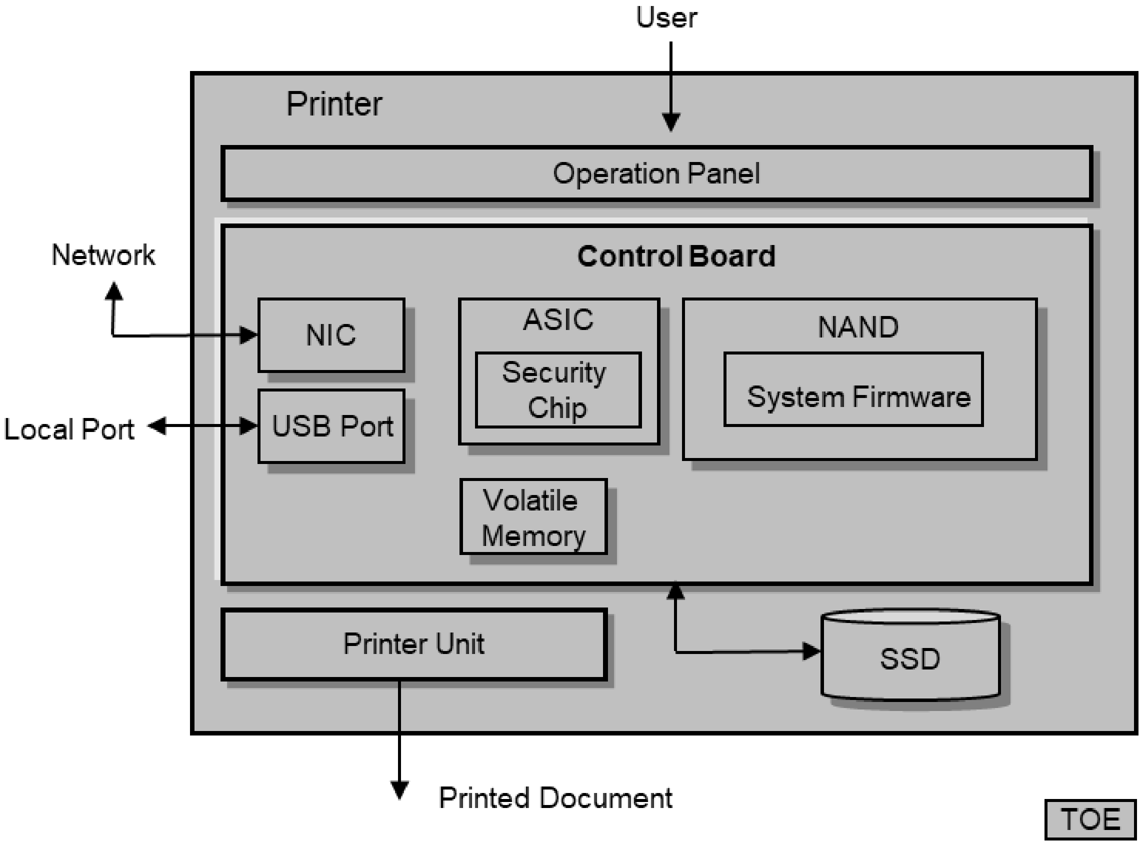

Figure 1. Physical configuration of the TOE

The TOE consists of an Operation Panel, 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 Printer Unit is the hardware that outputs printed material.

A Control Board is the circuit board to control the 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) and a Local Interface (USB Port).

An ASIC that is also on the Control 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 (TA Triumph-Adler/UTAX)

ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x First Steps Quick Guide

ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x Operation Guide

ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x Safety Guide

Data Encryption/Overwrite Operation Guide

Command Center RX User Guide

ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x 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 ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, and ECOSYS PA4500x models, with system firmware: C0T_S0IS.C04.002

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 2023-01-10 and 2023-02-09. The PA6000x model with system firmware C0T_S0IS.C04.002 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 2023-01-10 and 2023-01-12. The PA6000x model with system firmware C0T_S0IS.C04.002 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. 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, and a Microsoft Edge web browser
- Authentication server connected via IPSec with IKE1

In the evaluated configuration:

- a solid state disk drive HD-18 (SSD) 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 PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x Series with SSD Security Target, Kyocera Document Solutions Inc., 2023-02-09, document version 1.0, FMV ID 22FMV6373-10

Notice1 Notice (KYOCERA), Kyocera Document Solutions Inc., 2023-02, document version 3VC0T5655001, FMV ID 22FMV6373-10

Notice2 Notice (TA Triumph-Adler/UTAX), Kyocera Document Solutions Inc., 2023-02, document version 3VC0T5656001, FMV ID 22FMV6373-10

QG ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x First Steps Quick Guide, Kyocera Document Solutions Inc., 2022-06, document version 3VC0T5602001, FMV ID 22FMV6373-10

OG ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x Operation Guide, Kyocera Document Solutions Inc., 2022-08, document version C0TKDEN000, FMV ID 22FMV6373-10

SG ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x Safety Guide, Kyocera Document Solutions Inc., 2022-06, document version 3VC0T5622001, FMV ID 22FMV6373-10

DE Data Encryption/Overwrite Operation Guide, Kyocera Document Solutions Inc., 2023-03, document version 3MSC0TKDEN1, FMV ID 22FMV6373-10

CCRX Command Center RX User Guide, Kyocera Document Solutions Inc., 2022-09, document version C0TCCRXKDEN29, FMV ID 22FMV6373-10

PD ECOSYS PA6000x, ECOSYS PA5500x, ECOSYS PA5000x, ECOSYS PA4500x Printer Driver User Guide, Kyocera Document Solutions Inc., 2022-07, document version C0TBWKTEN820.2022.07 FMV ID 22FMV6373-10

NDP KYOCERA Net Direct Print User Guide, Kyocera Document Solutions Inc., 2022-09, document version DirectPrintKDEN4.2022.9, FMV ID 22FMV6373-10

EP-002 002 Evaluation and Certification, CSEC, 2021-Oct-26, document version 34.0

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, and Scheme Notes, have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.4	2023-06-15	None
2.3.2	2023-04-20	None
2.3	2023-01-26	None
2.2	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Subject	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