FMV

CSEC

Swedish Certification Body for IT Security

Certification Report - KYOCERA TASKalfa 3253ci, TASKalfa 2553ci Series with FAX System

Issue: 1.0, 2019-Dec-10

Authorisation: Ulf Noring, Lead Certifier , CSEC

Table of Contents

1   Executive Summary

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

Kyocera:
TASKalfa 3253ci
TASKalfa 2553ci
TASKalfa 3253ciG
TASKalfa 2553ciG

TA Triumph-Adler:
3207ci
2507ci

UTAX:
3207ci
2507ci

The TSF and its execution environment are the same in all the listed models above. The only differences between them are print speed and sales destinations. The following firmware is used by the system:

System Firmware: 2VG_S0IS.C01.013
FAX Firmware : 3R2_5100.003.012

The MFP models with fax system provide copying, scan to send, printing, faxing and box functionality.

The evaluated security features include user management, data access control, fax data flow control, solid state drive encryption, auditing, security management, self-test, and network protection (IPSec and TLS).

The following functionality is excluded from the evaluation:

- The maintenance interface
- Network authentication
- The installation of Java applications on the MFP

The Security Target does not claim conformance to any Protection Profile.

The TOE is delivered to the customer by a courier trusted by KYOCERA Document Solutions Inc. The main MFP printer unit is delivered separately from the FAX system add-on. The TOE can be purchased from a KYOCERA Document Solutions Inc. group corporation directly or from a dealer. A service person from the organisation that sold the TOE will set it up for the customer.

The evaluation has been performed by Combitech AB in their premises in Sundbyberg and Bromma, Sweden with testing done in the developer's premises in Osaka, Japan and was completed on the 8th of November 2019.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 5, and the Common Methodology for IT Security Evaluation, version 3.1, revision 5. The evaluation conforms to evaluation assurance level EAL 2, augmented by ALC_FLR.2.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Critera Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025:2005 for Common Criteria evaluation.

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 have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for the evaluation assurance level EAL 2 + 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	CSEC2018012
Name and version of the certified IT product	KYOCERA TASKalfa 3253ci/2553ci/3253ciG/2553ciG
	TA Triumph-Adler 3207ci/2507ci
	UTAX 3207ci/2507ci
	The FAX System 12 option for the above printer models
	System Firmware: 2VG_S0IS.C01.013 FAX Firmware : 3R2_5100.003.012
Security Target Identification	TASKalfa 3253ci, TASKalfa 2553ci Series with FAX System 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 revision 5
CEM version	3.1 revision 5
QMS version	1.23
Scheme Notes Release	14.0
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2019-12-XX

3   Security Policy

The TOE consists of eight security functions, listed below together with a short description of each function.

3.1   User Management

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. It also includes a function which protects feedback on input of login user password when performing identification and authentication as well as a function which automatically logs the user out in case no operation has been performed for a certain period of time.

3.2   Data Access Control

Restricts access so that only authorized users can access to image data stored in the TOE. Users who own boxes can give other users permission to view the contents of a particular box, and also set a password to further protect the box.

3.3   Fax Data Flow Control

Controls forwarding the data received from a public line to the TOE's external interface according to the configuration of the FAX forward setting.

3.4   Solid State Drive Encryption

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

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

The security management function allows only authorized users to edit user information, set the TOE security functions, and manage TSF. The Security management function can be performed from the Operation Panel and Client PCs. Web browser is used for operation from Client PCs.

3.7   Self-Test Function

The self-test function performs the following self-tests at TOE startup:

• Check if SSD encryption is correctly performed.

• Check the integrity of the generated encryption key

• Check the integrity of executable module of the security function

3.8   Network Protection Function

The network protection function encrypts all data in transit over the network between the TOE and trusted IT products and prevents unauthorized alteration and disclosure.

4   Assumptions and Clarification of Scope

4.1   Usage 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

5.1 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 the system firmware and fax firmware. The different parts are depicted in a diagram below.
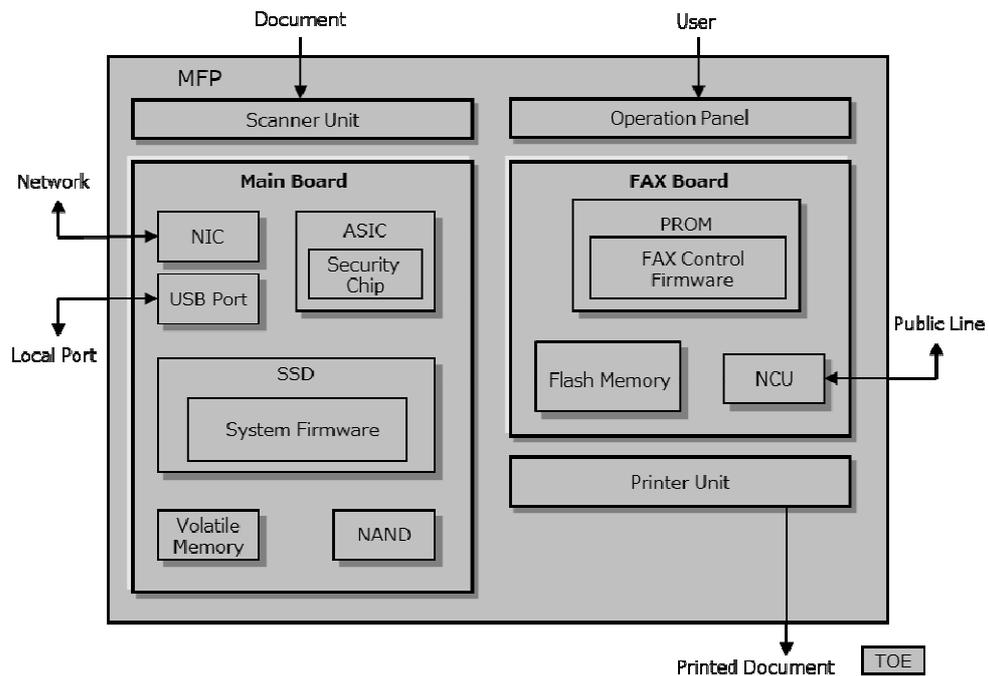
The Operation Panel is the hardware that displays status and results upon receipt of input by the TOE user. The Scanner and Printer units are the hardware that input documents into the TOE and output documents as printed material.

The Main Board is the circuit board that controls the 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). There is also an ASIC on the Main Board. The ASIC includes a Security Chip which implements security arithmetic processing for the SSD encryption function.

The FAX control firmware that controls FAX communication is installed on the PROM, which is positioned on the FAX Board. Additionally, the FAX Board has an NCU interface.

The NAND stores device settings while the Volatile Memory is used as working area.

The SSD that stores image data and job data is connected to the Main Board. Any of the above memory mediums are not removable. Only the FAX receive/send image is stored in the Flash Memory. Image data handled by other basic functions is stored on the SSD.

5.2 Logical configuration of the TOE

The below diagram illustrates the logical scope of the TOE:
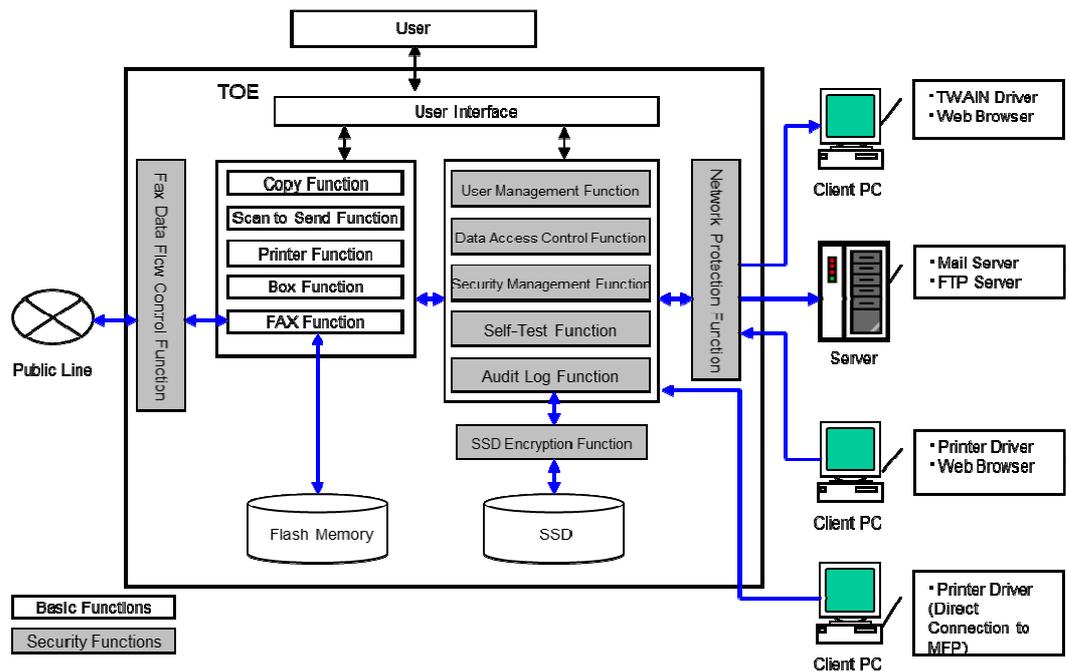
Please see section 1.4.3 in the [ST] for a more detailed description of the functionality shown in the diagram.

There is no interface for any user or administrator to directly interact with the TOE operating system, all interactions must go via one of the standard application functions or the hardware interfaces of the TOE.

6   Documentation

The following guidance documents are available:

[SG]

TASKalfa 2553ci / TASKalfa 3253ci / TASKalfa 4053ci / TASKalfa 5003i / TASK-alfa 5053ci / TASKalfa 6003i / TASKalfa 6053ci Safety Guide

[OG-ci]

TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3253ci, TASKalfa 2553ci Operation Guide

[OG-FAX]

FAX System 12 Operation Guide

[OG-DE]

Data Encryption/Overwrite Operation Guide

[UG-PR-ci]

TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3553ci / TASK-alfa 3253ci / TASKalfa 2553ci Printer Driver User Guide

[UG-CCRX]

Command Center RX User Guide

[IG-FAX]

FAX System 12 Installation Guide

[QG-ci]

TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3253ci / TASK-alfa 2553ci First Steps Quick Guide

[UG-DP]

KYOCERA Net Direct Print User Guide

[NOTICE]

Notice

7   IT Product Testing

7.1   Developer Testing

The developer performed extensive manual tests on the following printer models:

TASKalfa 3253ci
TASKalfa 2553ci

Since the TSF and its execution environment are the same in all the listed models above, and the only differences between them are print speed and sales destinations, this covers all of the TOE models listed in chapter 1.

The developer testing was done on the following firmware:

System Firmware: 2VG_S0IS.C01.013
FAXFirmware: 3R2_5100.003.012

The developer's testing covers the security functional behaviour of all TSFIs and most SFRs. Some gaps to the SFRs were identified and covered by evaluator independent testing. All test results were as expected. The testing was performed on the developer's premises in Osaka, Japan.
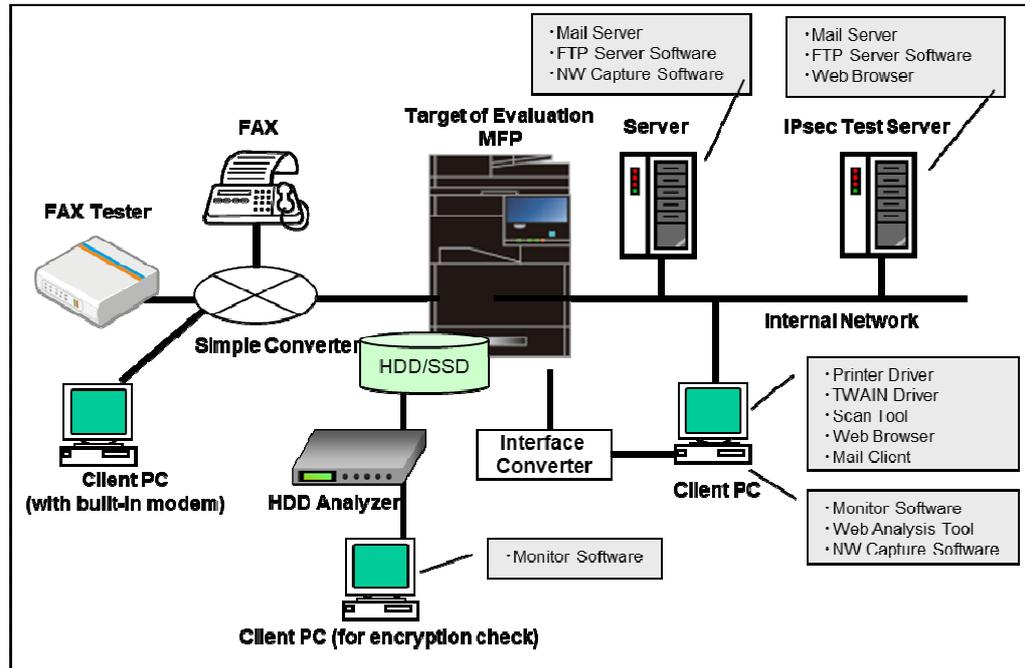
7.2   Evaluator Testing

The evaluator's independent tests were chosen to complement the developer's manual tests in order to complement the cover of the security functional behaviour of the SFRs. The evaluator repeated a sample of the developer's test cases and performed individual and penetration test cases. The tests included:

TOE Installation
Identification and Authentication
Job Authorization
Data Access Control
SSD Encryption
Audit Log
Security Management
Self Test
Network Protection

7.2.1   Test Environment

The evaluator performed the tests on the developer's premises in Osaka, Japan using the same test environment as the developer but only tested one hardware model, the TASKalfa 2553ci. This was accepted since all TOE models execute on the same main board with the same CPU running the same set of firmware. The test environment was set up according to the below diagram:

7.3   Penetration Testing

The evaluators penetration tested the TOE using the same test environment as described above in chapter 7.2.1. The following types of penetration tests were performed:

- Port scan

- Vulnerability scan including web application vulnerability scan

- JPG fuzzing

Port scans were run after installation and configuration had been done according the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned for TCP/UDP.

Nessus (www.tenable.com) basic network vulnerability scans were run. No high, medium, or low severity issues concerning the evaluated configuration were found.

A JPG picture was fuzzed approximate 110 times using the Peach fuzzing tool.

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

8   Evaluated Configuration

A notice [NOTICE] included with the TOE details verification procedures of the TOE, explains that use of applications on the TOE is not allowed in the evaluated configuration, and guides users to follow the Data Encryption/Overwrite Operation Guide [OG-DE] to configure the TOE. The Data Encryption/Overwrite Operation Guide [OG-DE] describes how to configure the TOE to reach evaluated configuration in the chapter named "After Installation". The instructions need to be followed in order to use the evaluated configuration.

8.1   Dependencies to Other Hardware, Firmware and Software

The TOE is the hardware and firmware of the various MFP models listed in chapter 1. To be fully operational, any combination of the following items may be connected to the MFP:

- A LAN for network connectivity.

- A telephone line for fax capability.

- IT systems that submit print jobs to the TOE via the network using standard print protocols.

- IT systems that send/and or receive faxes via the telephone line

- An SMTP server/FTP server/client PC/other FAX system/USB memory that will receive any input sent to the MFP if the MFP is configured to send it to them.

- A USB memory that can be used as an input source for print jobs (i.e. print from USB).

8.2   Excluded from TOE Evaluated Configuration

The following features of the TOE are outside of the evaluated configuration:

- The maintenance interface

- Network authentication

- Expanding functionality by installing Java applications is not allowed in the TOE evaluated configuration. The user manual [OG-ci] calls the Java applications "applications". More information can be found in chapter 5, "Application", in [OG-ci].

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 evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluator's overall verdict is PASS.

The verdicts for the assurance classes and components are summarized 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

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 Drive
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

12.1   General

CCp1   Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCp2   Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCp3   Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003

CEM   Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004

ST   TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASK-alfa 3553ci Series with FAX System, Security Target, KYOCERA Document Solutions Inc., 2019-11-08, document version 1.07

SP-002   SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

SP-188   SP-188 Scheme Crypto Policy, CSEC, 2019-09-25, document version 9.0

12.2   Documentation

SG   TASKalfa 2553ci / TASKalfa 3253ci / TASKalfa 4053ci / TASKalfa 5003i / TASKalfa 5053ci / TASKalfa 6003i / TASKalfa 6053ci Safety Guide, KYOCERA Document Solutions Inc., 2018-09, document version 302V85622001

OG-ci   TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3253ci, TASKalfa 2553ci Operation Guide, KYOCERA Document Solutions Inc., 2018-09, document version 2V8KDEN000

OG-FAX   FAX System 12 Operation Guide, KYOCERA Document Solutions Inc., 2018-09, document version 303RK5671006

OG-DE   Data Encryption/Overwrite Operation Guide, KYOCERA Document Solutions Inc., 2019-11, document version 3MS2V8GEEN3

UG-PR-ci TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3553ci / TASKalfa 3253ci / TASKalfa 2553ci Printer Driver User Guide, KYOCERA Document Solutions Inc., 2018-09, document version 2V8CLKTEN730

UG-CCRX   Command Center RX User Guide, KYOCERA Document Solutions Inc., 2018-09, document version CCRXKDEN17

IG-FAX   FAX System 12 Installation Guide, KYOCERA Document Solutions Inc., 2018-10, document version 303RK5671006

QG-ci   TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa

3253ci / TASKalfa 2553ci First Steps Quick Guide, KYOCERA Document Solutions Inc., 2018-09, document version 302V85602001

UG-DP   KYOCERA Net Direct Print User Guide, KYOCERA Document Solutions Inc., 2016-02, document version DirectPrintKDEN1

NOTICE   Notice, KYOCERA Document Solutions Inc., 2019-11, document version 302VK5641004

Appendix A   Scheme Versions

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

A.1   Scheme/Quality Management System

Version	Introduced	Impact of changes
1.23	2019-10-14	None
1.22.3	2019-05-20	None
1.22.2	2019-05-02	None
1.22.1	2019-03-08	None
1.22	2019-02-01	None
1.21.5	Application	Original version

A.2   Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL2: evaluator + developer tests together provide full coverage of the TSFI.
SN-18	1.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	1.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.