Ärendetyp 5.3 Diarienummer: 24FMV6695-42

Dokument ID CSEC2024023

Swedish Certification Body for IT Security

Certification Report Kyocera TASKalfa MZ2501ci HCDPP

Issue: 1.0, 2026-feb-26

Authorisation: Michael Lindh Almér, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

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

- KYOCERA TASKalfa MZ3501ci
- KYOCERA TASKalfa MZ2501ci
- KYOCERA TASKalfa M30135ci
- KYOCERA TASKalfa M30125ci
- TA Triumph-Adler 3509ci
- TA Triumph-Adler 2509ci
- UTAX 3509ci
- UTAX 2509ci

With the system firmware C2L_S000.001.226 and FAX System 14.

In the evaluated configuration, the optional fax board is installed and included in the scope of the TOE. The TOE provides copying, scanning, printing, faxing and boxing.

Delivery is done by means of a courier trusted by KYOCERA Document Solutions Inc. Installation and initial setup is done by a representative of KYOCERA.

The ST claims exact conformance to the Protection Profile for Hardcopy Devices (HCDPP) v1.0, including Errata #1.

The evaluation has been performed by Combitech AB, in their premises in Bromma, Sweden, and was completed on the January 8 2026.

The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 revision 5, Common Evaluation Methodology (CEM), version 3.1 revision 5, and the HCDPP v1.0 including Errata #1. 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), the Common Methodology for evaluation assurance level EAL 1 augmented by ASE_SPD.1, and the HCDPP v1.0 including Errata#1.

The technical information in this report is based on the Final Evaluation Report (FER) produced by Combitech AB, and the Security Target (ST).

> 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	CSEC2024023
Name and version of the certified IT product	KYOCERA TASKalfa MZ3501ci, TASKalfa MZ2501ci, TASKalfa M30135ci, TASKalfa M30125ci (KYOCERA), 3509ci, 2509ci (TA Triumph-Adler/UTAX), with FAX System With system firmware C2L_S000.001.226 and FAX System 14
Security Target Identification	HCD-PP_TASKalfa MZ3501ci, TASKalfa MZ2501ci Series with FAX System Security Target, 2026-01-07, version 1.02
EAL	EAL 1 + ASE_SPD.1 Exact conformance to the Protection Profile for Hardcopy Devices (HCDPP) v1.0, including Errata #1
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	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2026-02-26

3 Security Policy

The TOE provides the following security services:

- User Management
- Data Access Control
- Job Authorization
- SSD Encryption
- Audit Log
- Security Management
- Trusted Operation
- Network Protection
- PSTN Fax-Network Separation

3.1 User Management

User management function is a function that identifies and authenticates whether persons are authorized users when users intend to operate the TOE from the operation panel or the client PCs. For identification authentication, TOE obtains the login user name and login password from the user, performs identification authentication using the local authentication method, and permits the operation of TOE only to users who are determined to be authorized users as a result of verification.

When the TOE is used from the Operation Panel or a Web browser, the login screen is displayed and a user is required to enter his or her login user name and login password.

When the TOE is accessed from the printer driver or TWAIN driver, the TOE identifies and authenticates if the person is authorized by referring to the login user name and login user password obtained from a user job.

3.2 Data Access Control

The data access control function is a function that allows authorized users only to access to image data and job data stored in the TOE using each of the TOE basic function such as copy, scan to send, print, fax and box function.

3.3 Job Authorization

The job authorization function is a function that allows authorized users only to use the TOE basic function such as copy, scan to send, print, fax and box function.

3.4 SSD Encryption

Once the basic function of the TOE is executed, image data, job data and TSF data is stored on the SSD. The SSD encryption function is a function that encrypts data and then stores the data on the SSD when storing these data on the SSD.

3.5 Audit Log

The audit log function is a function that generates, records and sends to Audit Log server the audit logs when occurring auditable events.

3.6 Security Management

Security management function is a function that allows authorized users only to edit user information, set the TOE security functions and manage. 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 Trusted Operation

In Trusted operation, a firmware version check function and a function for permitting firmware update are provided to the administrators, and a function for executing the following self-test at the start-up of TOE is provided.

3.8 Network Protection

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

3.9 PSTN Fax-Network Separation

TOE ensure separation between the PSTN fax line and the Internal Network.

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.PHYSICAL
  Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment
- A.NETWORK
  The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
- A.TRUSTED_ADMIN
  TOE Administrators are trusted to administer the TOE according to site security policies.
- A.TRAINED_USERS
  Authorized Users are trained to use the TOE according to site security policies.

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation.

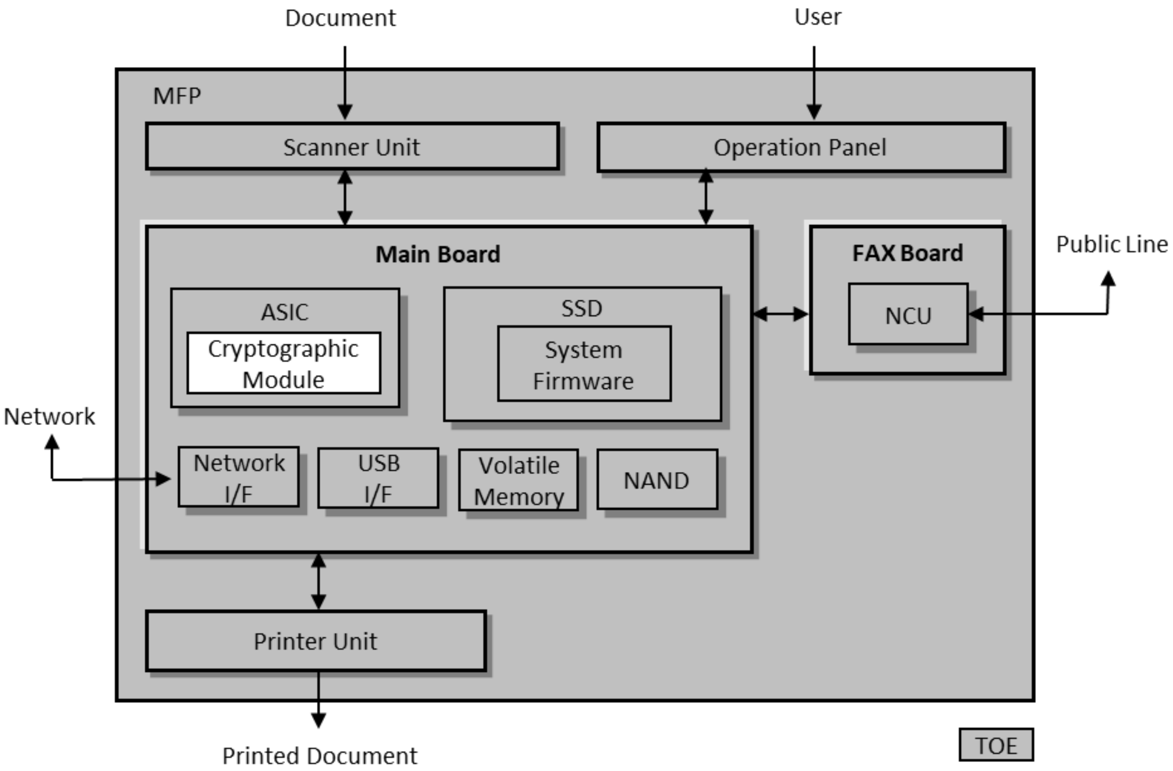
- T.UNAUTHORIZED_ACCESS
  An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE’s interfaces.
- T.TSF_COMPROMISE
  An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE’s interfaces.
- T.TSF_FAILURE
  A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
- T.UNAUTHORIZED_UPDATE
  An attacker may cause the installation of unauthorized software on the TOE.
- T.NET_COMPROMISE
  An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

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

- P.AUTHORIZATION
  Users must be authorized before performing Document Processing and administrative functions.
- P.AUDIT
  Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
- P.COMMS_PROTECTION
  The TOE must be able to identify itself to other devices on the LAN.

- P.STORAGE_ENCRYPTION
  If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
- P.KEY_MATERIAL
  Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
- P.FAX_FLOW
  If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
- P.PURGE_DATA
  The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Non-volatile Storage Devices.

5 Architectural Information



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 an SSD, which is positioned on the Main Board. The Main Board has a Network Interface and a USB Interface.

The ASIC on the Main Board is installed with a cryptographic module to perform the SSD encryption function (See below). A FIPS 140-2 certified cryptographic module, key derivation and entropy are provided by this cryptographic module in TOE environment.

A FAX Board has a Public Line Interface (NCU) as an interface.

As for memory mediums, a NAND that stores device settings, a Volatile Memory that is used as working area and an SSD for the system firmware installation or image data are positioned on the Main Board. Any of the above memory mediums are not removable. Image data handled by other basic functions is stored in the SSD.

6 Documentation

The following guidance documents are part of the TOE:

Document name	Version
ISO 15408 Notice (KYOCERA)	C2LHCDPPKD01
ISO 15408 Notice (KYOCERA)	C2LIEEEKR01
ISO 15408 Notice (TA Triumph-Adler/UTAX)	C2LIEEEGE01
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i First Steps Quick Guide (KYOCERA)	3VC2G5601001
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Operation Guide (KYOCERA)	C2GKDEN002
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Safety Guide (KYOCERA)	3VC2G5622001
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i FAX Operation Guide	C2GKDEN501
Data Encryption/Overwrite Operation Guide	3MSC2GKDEN01
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Command Center RX User Guide	C2GCCRXKDEN32
TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Printer Driver User Guide (KYOCERA)	C2GCLKTEN842
KYOCERA Net Direct Print User Guide	DirectPrintKDEN7

7 IT Product Testing

7.1 Evaluator Testing

All TOE variants included in the evaluation use the same firmware: C2L_S000.001.226, and execute on the same main board with the same processor. The TASKalfa MZ3501ci model was used for testing, representing all TOE variants.

All the test cases defined in the HCDPP were performed. The testing took place in Combitech's premises in Bromma, Sweden, between 2025-10-10 and 2025-10-20.

All tests were successful and no errors were discovered.

7.2 Penetration Testing

The TASKalfa MZ3501ci model was used for penetration testing.

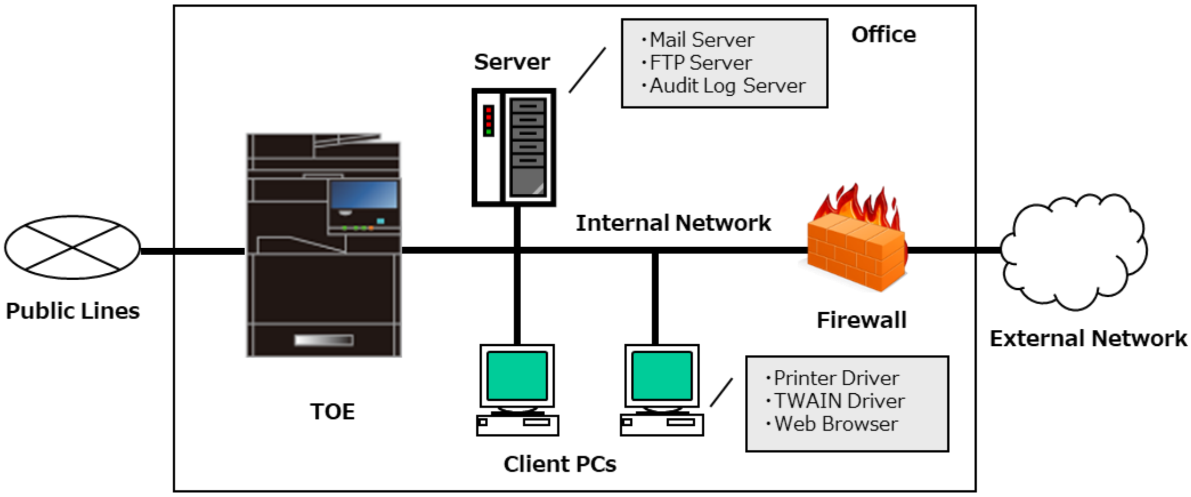
The evaluators performed port scans (NMAP), vulnerability scan (Nessus), and jpeg fuzz tests (Peach).

The testing took place in Combitech's premises in Bromma, Sweden, between 2025-10-18 and 2025-10-20.

No vulnerabilities were found during the penetration testing.

8 Evaluated Configuration

Normal user environment.



Required Non-TOE Hardware, Software and Firmware name is as follows.

- Client PCs: IPsec (IKEv1) should be available.
  - Printer Driver: KX Driver
  - TWAIN Driver: Kyocera TWAIN Driver
  - Web Browser: Microsoft Edge
- Mail Server: IPsec (IKEv1) should be available.
- FTP Server: IPsec (IKEv1) should be available.
- Audit Log Server (syslog server): IPsec (IKEv1) should be available.
- Cryptographic module: Kyocera MFP Cryptographic Module(A) should be available.
  - Hardware version: 2.1.10
  - CAVP Validation Number: C1892
- Cryptographic module for FDE: Kyocera MFP Cryptographic Module(A) – FDE should be available.
  - Hardware version: 2.3
  - CAVP Validation Number: C1933

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:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Functional Specification	ADV_FSP.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.1	PASS
CM Scope	ALC_CMS.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Extended Component Definition	ASE_ECD.1	PASS
Security Objectives	ASE_OBJ.1	PASS
Security Requirements	ASE_REQ,1	PASS
Security Problem Definition	ASE_SPD.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Independent Testing	ATE IND.1	PASS
Vulnerability Analysis	AVA	PASS
Vulnerability Analysis	AVA_VAN.1	PASS
The assurance activities in the HCDPP v1.0 including Errata #1	-	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 Disk
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

ST	HCD-PP TASKalfa MZ3501ci, TASKalfa MZ2501ci Series with FAX System Security Target Version 1.02, KYOCERA Document Solutions Inc, Combitech AB, 2026-01-07, FMV ID 24FMV6695-49
N1	ISO 15408 Notice (KYOCERA), 2025-08, C2LHCDPPKD01
N2	ISO 15408 Notice (KYOCERA), 2025-08, C2LIEEEKR01
N3	ISO 15408 Notice (TA Triumph-Adler/UTAX), 2025-08, C2LIEEEGE01
QG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i First Steps Quick Guide (KYOCERA), 2024-06, 3VC2G5601001
OG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Operation Guide (KYOCERA), 2024-11, C2GKDEN002
SG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Safety Guide (KYOCERA), 2024-06, 3VC2G5622001
FAX-OG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i FAX Operation Guide, 2025-01, C2GKDEN501
DE-OOG	Data Encryption/Overwrite Operation Guide, 2025-09, 3MSC2GKDEN01
UG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci / TASKalfa MZ7001i / TASKalfa MZ6001i / TASKalfa MZ5001i / TASKalfa MZ4001i Command Center RX User Guide, 2024-12, C2GCCRXKDEN32
PD-UG	TASKalfa MZ7001ci / TASKalfa MZ6001ci / TASKalfa MZ5001ci / TASKalfa MZ4001ci / TASKalfa MZ3501ci / TASKalfa MZ2501ci Printer Driver User Guide (KYOCERA), 2025-04, C2GCLKTEN842
DP	KYOCERA Net Direct Print User Guide, 2025-03, DirectPrintKDEN7

HCDPP Protection Profile for Harcopy Devices, IPA, NIAP and MFP Technical Community, 2015-09-10, document version 1.0, (including Errata #1, June 2017)

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003

CC CCpart1 + CCPart2 + CCPart3

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

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
2.6.1	2025-10-16	No impact
2.6	2025-04-23	No impact
2.5.2	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on the Security Target	Compliant
SN-22	4.0	Vulnerability assessment	Compliant
SN-25	2.0	Use of CAVP-tests in CC evaluations	Compliant
SN-27	1.0	ST requirements at the time of application for certification	Compliant
SN-28	2.0	Updated procedures for application, evaluation and certification	Compliant