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

Issue: 1.0, 2019-Dec-10

Authorisation: Ulf Noring, Lead Certifier, CSEC
Table of Contents

1 Executive Summary 4
2 Identification 7
3 Security Policy 8
   3.1 User Management 8
   3.2 Data Access Control 8
   3.3 Job Authorization Function 8
   3.4 Hard Disk Drive Encryption 8
   3.5 Overwrite-Erase Function 8
   3.6 Audit Log 8
   3.7 Security Management 8
   3.8 Self-Test Function 9
   3.9 Network Protection Function 9
4 Assumptions and Clarification of Scope 10
   4.1 Usage Assumptions 10
   4.2 Clarification of Scope 10
5 Architectural Information 12
   5.1 Physical configuration of the TOE 12
   5.2 Logical configuration of the TOE 13
6 Documentation 14
7 IT Product Testing 15
   7.1 Developer Testing 15
   7.2 Evaluator Testing 15
   7.3 Penetration Testing 16
8 Evaluated Configuration 17
   8.1 Dependencies to Other Hardware, Firmware and Software 17
   8.2 Excluded from TOE Evaluated Configuration 17
9 Results of the Evaluation 18
10 Evaluator Comments and Recommendations 19
11 Glossary 20
12 Bibliography 21
   12.1 General 21
   12.2 Documentation 21
Appendix A Scheme Versions 23
   A.1 Scheme/Quality Management System 23
   A.2 Scheme Notes 23
1 Executive Summary

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

**Kyocera:**
- TASKalfa 3253ci
- TASKalfa 2553ci
- TASKalfa 3253ciG
- TASKalfa 2553ciG

**Copystar:**
- CS 3253ci
- CS 2553ci

**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_S01S.C01.013
- **FAX Firmware:** 3R2_5100.003.012

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

The evaluated security features include user management, data access control, job authorization, hard drive encryption, overwrite-erase functionality, 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 ST claims demonstrable conformance to the following PP:
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 TOE claims conformance to the following SFR packages:

- 2600.2-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment B Conformant
- 2600.2-SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment B Conformant
- 2600.2-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment B Conformant
- 2600.2-FAX SFR Package for Hardcopy Device Fax Functions, Operational Environment B Conformant
- 2600.2-DSR SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B Conformant
- 2600.2-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B Conformant

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 Hard Disk and FAX system add-ons. 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 Criteria 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

<table>
<thead>
<tr>
<th>Certification Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification ID</td>
</tr>
<tr>
<td>Name and version of the</td>
</tr>
<tr>
<td>certified IT product</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Security Target Identification</td>
</tr>
<tr>
<td>EAL</td>
</tr>
<tr>
<td>Sponsor</td>
</tr>
<tr>
<td>Developer</td>
</tr>
<tr>
<td>ITSEF</td>
</tr>
<tr>
<td>Common Criteria version</td>
</tr>
<tr>
<td>CEM version</td>
</tr>
<tr>
<td>QMS version</td>
</tr>
<tr>
<td>Scheme Notes Release</td>
</tr>
<tr>
<td>Recognition Scope</td>
</tr>
<tr>
<td>Certification date</td>
</tr>
</tbody>
</table>
3 Security Policy

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

3.1 User Management
Identifies and authenticates whether persons are authorized users when users intend to operate the TOE from the operation panel or client PCs.
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 the job sent by the user.

3.2 Data Access Control
Allows authorized users to only access their own image 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. 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 Job Authorization Function
Allows only authorized users to use the TOE basic function such as copy, scan to send, print, fax and box function.

3.4 Hard Disk Drive Encryption
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
After each basic function (such as scanning, printing, etc.) completes, the TOE deletes used image data on the HDD or flash memory. When deleting stored image data on the HDD, the overwrite-erase function overwrites the actual image data with meaningless character strings so that it disables re-usage of the data.

3.6 Audit Log
The audit log function generates, records and manages audit logs when auditable events occur.

3.7 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.
3.8 **Self-Test Function**

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

- Check if HDD encryption is correctly performed.
- Check the integrity of the generated encryption key
- Check the integrity of executable module of the security function

3.9 **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. This function also provides a feature to prevent forwarding of information from an external interface to an internal network through the TOE without permission.
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.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
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

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, HDD and SSD hardware, and the system firmware and fax firmware. The different parts are depicted in a diagram below.

![Diagram of TOE components]

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 HDD encryption function and HDD Overwrite-Erase 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 HDD 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 HDD. Image data is not 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]

[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]

[UG-CCRX]
Command Center RX User Guide

[IG-FAX]
FAX System 12 Installation Guide

[IG-HD]
HD-12 Installation Guide

[QG-ci]
TASKalfa 6053ci / TASKalfa 5053ci / TASKalfa 4053ci / TASKalfa 3253ci / TASKalfa 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
- HDD Encryption/Overwrite-Erase
- 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 approximately 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:

<table>
<thead>
<tr>
<th>Assurance Class Name / Assurance Family Name</th>
<th>Short name (including component identifier for assurance families)</th>
<th>Verdict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Target Evaluation</td>
<td>ASE</td>
<td>PASS</td>
</tr>
<tr>
<td>ST Introduction</td>
<td>ASE_INT.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Conformance claims</td>
<td>ASE_CCL.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Security Problem Definition</td>
<td>ASE_SPD.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Security objectives</td>
<td>ASE_OBJ.2</td>
<td>PASS</td>
</tr>
<tr>
<td>Extended components definition</td>
<td>ASE_ECD.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Derived security requirements</td>
<td>ASE_REQ.2</td>
<td>PASS</td>
</tr>
<tr>
<td>TOE summary specification</td>
<td>ASE_TSS.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC</td>
<td>PASS</td>
</tr>
<tr>
<td>Use of a CM system</td>
<td>ALC_CMC.2</td>
<td>PASS</td>
</tr>
<tr>
<td>Parts of the TOE CM Coverage</td>
<td>ALC_CMS.2</td>
<td>PASS</td>
</tr>
<tr>
<td>Delivery procedures</td>
<td>ALC_DEL.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Flaw reporting procedures</td>
<td>ALC_FLR.2</td>
<td>PASS</td>
</tr>
<tr>
<td>Development</td>
<td>ADV</td>
<td>PASS</td>
</tr>
<tr>
<td>Security architecture description</td>
<td>ADV_ARC.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Security-enforcing functional specification</td>
<td>ADV_FSP.2</td>
<td>PASS</td>
</tr>
<tr>
<td>Basic design</td>
<td>ADV_TDS.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Guidance documents</td>
<td>AGD</td>
<td>PASS</td>
</tr>
<tr>
<td>Operational user guidance</td>
<td>AGD_OPE.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Preparative procedures</td>
<td>AGD_PRE.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE</td>
<td>PASS</td>
</tr>
<tr>
<td>Evidence of coverage</td>
<td>ATE_COV.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Functional testing</td>
<td>ATE_FUN.1</td>
<td>PASS</td>
</tr>
<tr>
<td>Independent testing - sample</td>
<td>ATE_IND.2</td>
<td>PASS</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>AVA</td>
<td>PASS</td>
</tr>
<tr>
<td>Vulnerability analysis</td>
<td>AVA_VAN.2</td>
<td>PASS</td>
</tr>
</tbody>
</table>
Evaluator Comments and Recommendations
None
11 **Glossary**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEM</td>
<td>Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITSEF</td>
<td>IT Security Evaluation Facility, test laboratory licensed to operate within an evaluation and certification scheme</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MFP</td>
<td>Multi-Function Printer</td>
</tr>
<tr>
<td>NCU</td>
<td>Network Control Unit</td>
</tr>
<tr>
<td>OSP</td>
<td>Organizational Security Policy</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transport Protocol</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>ST</td>
<td>Security Target, document containing security requirements and specifications, used as the basis of a TOE evaluation</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation</td>
</tr>
<tr>
<td>TSF</td>
<td>TOE Security Functionality</td>
</tr>
<tr>
<td>TSFI</td>
<td>TSF Interface</td>
</tr>
</tbody>
</table>
12 Bibliography

12.1 General


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


CCEVS-PL20 NIAP policy for the use of IEEE Multifunction Function Device Protection Profiles (IEEE 2600.1 and IEEE 2600.2), National Information Assurance Partnership (NIAP), 2010-11-15

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


<table>
<thead>
<tr>
<th>Document Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTICE</td>
<td>Notice, KYOCERA Document Solutions Inc., 2019-11, document version 302VK5641004</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Impact of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.23</td>
<td>2019-10-14</td>
<td>None</td>
</tr>
<tr>
<td>1.22.3</td>
<td>2019-05-20</td>
<td>None</td>
</tr>
<tr>
<td>1.22.2</td>
<td>2019-05-02</td>
<td>None</td>
</tr>
<tr>
<td>1.22.1</td>
<td>2019-03-08</td>
<td>None</td>
</tr>
<tr>
<td>1.22</td>
<td>2019-02-01</td>
<td>None</td>
</tr>
<tr>
<td>1.21.5</td>
<td>Application</td>
<td>Original version</td>
</tr>
</tbody>
</table>

A.2 Scheme Notes

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