SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-130 CR Certification Report

Issue 1.0 10 February 2026

Expiry date 10 February 2031

Trusted Security Filter (TSF) 201

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE ST 009E VERSION 2.5 15.05.2018

SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

Certification Statement

Trusted Security Filter (TSF) 201 allows secure data transfer between different security levels.

TSF 201 has been evaluated under the terms of the Norwegian Certification Authority for IT Security [10] and has met the Common Criteria Part 3 (ISO/IEC 15408) [3] conformant components of Evaluation Assurance Level (EAL) 5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 (ISO/IEC 15408) [2] conformant functionality in the specified environment when running on the platforms specified in Annex A.

The evaluation addressed the security functionality claimed in the ST Lite [12] with reference to the assumed operating environment specified by the ST Lite [12]. The evaluated configuration was that specified in Chapters 1, 2 and Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

Certifier	Øystein Hole, SERTIT
Date approved	10 February 2026
Expiry date	10 February 2031

1 Executive Summary

Prospective consumers are advised to read this report in conjunction with the ST Lite [12] which specifies the functional, environmental and assurance evaluation components.

The version of the product evaluated was TSF 201, comprising HW version 3AQ 25960 BAAA rev. F, SW version rev 2.8 build 0157.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thales Norway AS.

The TOE is a contents-filtering gateway consisting of both hardware and software. The purpose is to reject unwanted traffic by certain rules defined in a filter configuration file. It enables data transfer in a secure manner between two IP networks of different security classifications. Its design shall be trusted to perform separation of data between a HIGH (high security classification) network and a LOW (low security classification) network in a way upholding the security policy concerning data export and import between the individual networks. The TOE can be configured as a data diode that only allows data transfer from the LOW network to the HIGH network and blocks all data transfer in the other direction. Conversely, the TOE can be configured to block all data from the LOW network to the HIGH network.

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, six assumptions are made in the ST Public [12]. In order to counter seven threats as described in the ST Public [12], the TOE relies on the assumptions made. Details can be found in Chapter 3 Assumptions and Clarification of Scope.

The evaluation was performed by the ITSEF Nemko System Sikkerhet AS. The evaluation was performed in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in the document SD001E [10], as well as the Common Criteria (CC) Part 3 [3] and the Common Methodology for Information Technology Security Evaluation (CEM) [6].

The evaluation was performed at the assurance level EAL 5 augmented with ALC_FLR.3.

Nemko System Sikkerhet AS is an authorised ITSEF under the Norwegian Certification Authority for IT Security (SERTIT). Nemko System Sikkerhet AS is an accredited ITSEF according to the standard ISO/IEC 17025 for Common Criteria evaluation. The sponsor for this evaluation was Thales Norway AS.

The evaluation activities were monitored by the certification body. The security claims stated in the ST [11] was confirmed during the evaluation for the selected assurance level.

The basis for producing this Certification Report is the ST Lite [12] and the ETR [13].

2 TOE overview and Security Policy

The TOE is a contents-filtering gateway consisting of both hardware and software. The purpose is to reject unwanted traffic by certain rules defined in a filter configuration file.

It enables data transfer in a secure manner between two IP networks of different security classifications. Its design shall be trusted to perform separation of data between a HIGH (high security classification) network and a LOW (low security classification) network in a way upholding the security policy concerning data export and import between the individual networks.

It is designed for use in a highly specialized IT environment.

The TOE can be configured as a data diode that only allows data transfer from the LOW network to the HIGH network and blocks all data transfer in the other direction. Conversely, the TOE can be configured to block all data from the LOW network to the HIGH network.

The TOE records auditable events in an audit log that is protected from change and deletion. It can be viewed by authorized users.

The TOE has cryptographic functions to decrypt filter configuration files, software update files, and to encrypt and decrypt imported keys for internal use.

The TOE has an emergency erase function to securely delete cryptographic keys and filter configuration files.

The TOE has extensive self-test functions to support a fail secure design where single faults shall not violate the trusted functionality.

The TOE has tampering detection and also passive protection in terms of tampering seals. The electronic tampering detection will trigger emergency erase.

TSF 201 is TEMPEST certified. TEMPEST certification is outside the scope of the evaluation described in this document.

The TOE has an alarm indication for if a hardware or software failure is detected.

The TOE has a secure channel for connecting to its local management.

Figure 1 shows a schematic example of how the TOE may be deployed in an IP based system.

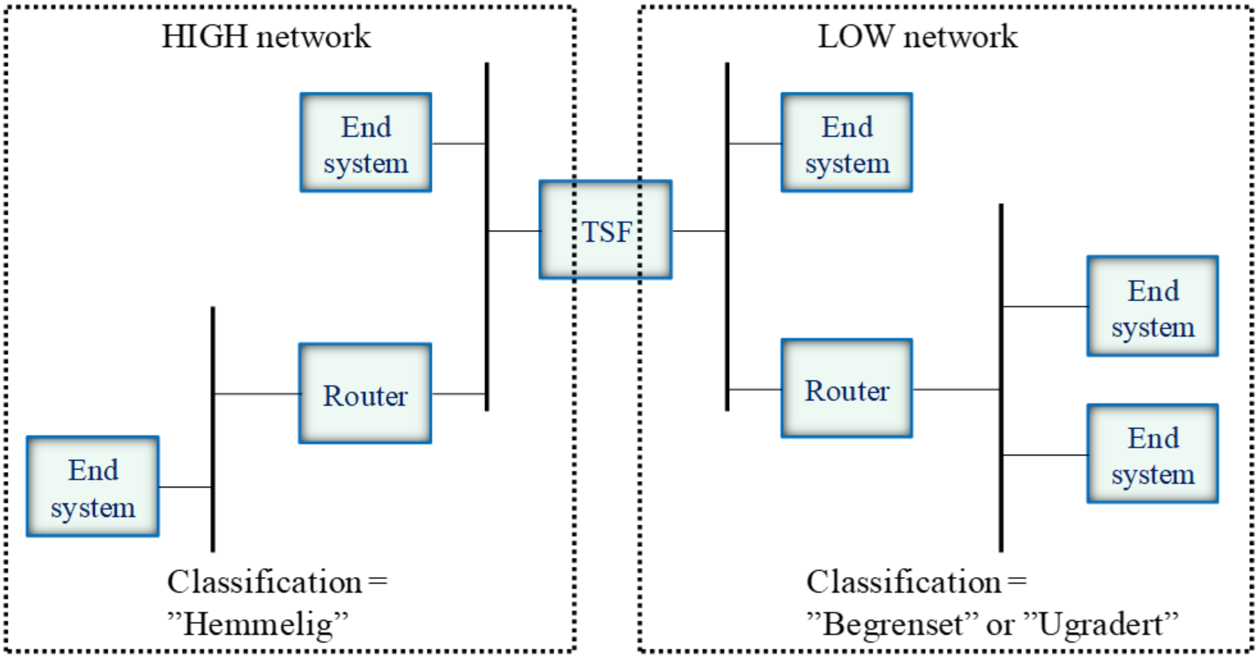

Figure 1

The TOE may typically permit all UDP and TCP traffic from the low classification system to the high classification system, and permit filtered UDP and TCP traffic from the high classification system to the low classification system. When TCP traffic is disabled, only UDP traffic shall be permitted. Traffic using other transport protocols than UDP and TCP will not be allowed to pass through the TOE. However, it is possible to block all traffic from the low classification to the high classification. The filter will reject messages that do not comply with the rules set by the filter configuration file.

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following six assumptions made regarding the usage and the operational environmental environment of the TOE are:

- PHYSICAL
- TRAINING
- CLEARANCE
- MAN_AUTHORISED
- USAGE
- ORGANIZATION

For details on these assumptions, the reader is advised to look at chapter 3.2 in the ST Lite [12].

3.2 Threats Countered

The threats and threat agents met by the TOE are diverse and depend on where the TOE is deployed. The following seven threats are countered by the TOE:

- CONN.HIGH.LOW
- TAMPERING
- MISUSE
- TEMPEST
- UNAUTHORIZED.USE
- ILLEGAL.CONFIG
- SECURE.KEY

For details on these threats, the reader is advised to look at chapter 3.5 in the ST Lite [12]. The reader should also have a look at the description of the threat agents in chapter 3.4 in the ST Lite [12].

3.3 Threats Countered by the TOE environment

There are no threats countered by the environment.

3.4 Organisational Security Policies

No organizational security policies were used in the evaluation.

4 Vulnerability Analysis and Testing

4.1 Vulnerability Analysis

The evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The search for publicly known vulnerabilities was conducted on 07 November 2025.

No exploitable vulnerabilities were found, but see chapter 7 in this report for recommendations for secure usage of the TOE.

4.2 Developer’s Tests

The evaluation showed that the Developer has thoroughly tested the TOE Security Functionality Interfaces (TSFI) and TSF modules of the TOE, and the test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. The developer has tested all the TSF subsystems, all the SFR-enforcing modules, and all the SFR-supporting modules against the TOE design and the security architecture description.

4.3 Evaluators’ Tests

The evaluators performed independent testing of a subset of the TSFIs and the TSF modules and verified that the TOE behaves as specified in the design documentation. Confidence in the developer's test results were gained by performing a sample of the developer's tests.

The evaluators devised penetration tests, based on the independent search for potential vulnerabilities and the security functions from the ST.

Testing was conducted in the week of 08-12 December 2025.

5 Evaluated Configuration

The evaluated TOE, as described in chapters 1, 2 and Annex A, is SW and HW. The TOE is delivered as a physical unit with SW installed. Filters must be built and installed in order for the TOE to operate as intended.

Installation of the TOE must be performed completely in accordance with the guidance documents [14] provided by the developer. The TOE should be used in the operational environment as specified in the ST Lite [12], as well as the guidance documents referenced in this chapter.

6 Evaluation Results

The evaluation addressed the requirements specified in the ST Lite [12]. The ITSEF reported the results of this work in the ETR [13] on the 12 February 2024.

The evaluators examined the following assurance classes and components taken from CC Part 3 [3]. These classes comprise the EAL 5 assurance package augmented with ALC_FLR.3.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
	ALC_FLR.3	Systematic flaw remediation
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification

Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

After due consideration of the ETR [13], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the certification team, SERTIT has determined that TSF 201, comprising HW version 3AQ 25960 BAAA rev. F, SW version rev 2.8 build 0157, meets the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on platforms specified in Annex A.

7 Recommendations

Prospective consumers of TSF 201 should understand the specific scope of the certification by reading this report in conjunction with the ST Lite [12]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST Lite [12].

The TOE should be installed and operated in accordance with the supporting guidance documentation [14] included in the evaluated configuration.

There were no other specific remarks or recommendations given by the evaluation team.

8 Security Target

The complete Security Target [11] used for the evaluation performed is sanitised for the purpose of publishing. The Public version (Security Target Lite [12]) is provided as a separate document. Sanitisation was performed according to the CCRA framework – ST sanitising for publication [7].

9 Glossary

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CDS	Cross Domain Solution
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
ITSEF	IT Security Evaluation Facility under the Norwegian Certification Scheme
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

10 References

[1] CC:2022, *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2022-11-001, Revision 1, CCRA, November 2022.

[2] CC:2022, *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2022-11-002, Revision 1, CCRA, November 2022.

[3] CC:2022, *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB-2022-11-003, Revision 1, CCRA, November 2022.

[4] CC:2022, *Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities*, CCMB-2022-11-004, Revision 1, CCRA, November 2022.

[5] CC:2022, *Common Methodology for Information Technology Security Evaluation, Pre-defined packages of security requirements*, CCMB-2022-11-005, Revision 1, CCRA, November 2022.

[6] CEM:2022, *Common Methodology for Information Technology Security Evaluation*, CCMB-2022-11-006, Revision 1, CCRA, November 2022.

[7] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.

[8] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[9] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[10] SERTIT (2020), *The Norwegian Certification Scheme*, SD001E, Version 10.5, SERTIT, 03 December 2020.

[11] Security Target for TSF 201, Rev 008, 17 December 2025

[12] Security Target for TSF 201 Lite, Rev 008-lite, 05 February 2026

[13] Evaluation Technical Report for TSF 201, version 1.2, 09 February 2026.

[14] Trusted Security Filter TSF 201 User Guide, Edition 5, 17 December 2025

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

TSF 201; comprising: HW version 3AQ 25960 BAAA rev. F, SW version rev 2.8 build 0157

Refer to the manufacturer’s documentation for additional information.

TOE Documentation

The supporting guidance documents evaluated were:

Trusted Security Filter TSF 201 User Guide, Edition 5

TOE Configuration

The testbed 1 was used for all testing of the TOE, while the testbed 2 was only used for sample testing of the TOE.

Testbed 1 was used e.g. for testing of TSF filter 1 (Diode) and TSF filters 2, 3 and 10 when the red traffic PC was on the same subnet as the TSF secure interface.

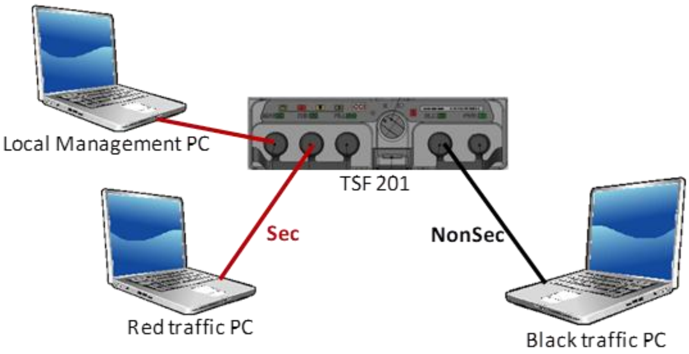

Figure 2 - Testbed 1

Testbed 2 was used e.g. for testing TSF Filter 1 (Diode) and new TSF filters when the red traffic PC was on a different subnet than the TSF secure interface.

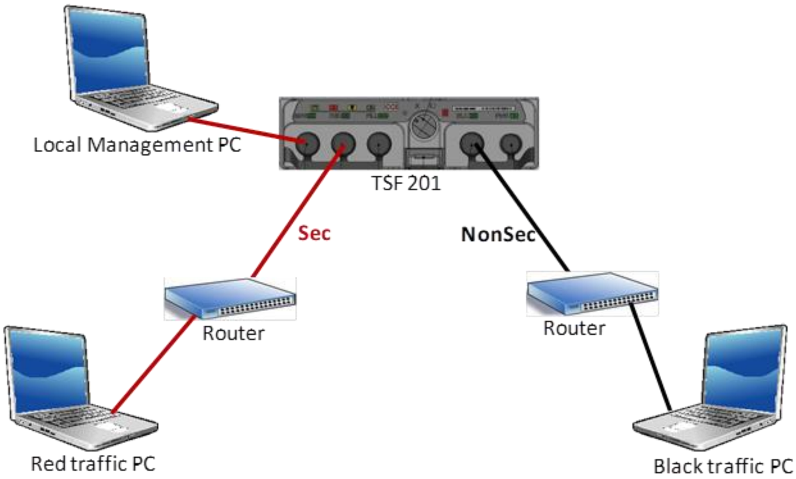

Figure 3 - Testbed 2