SERTIT

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

SERTIT-129 CR Certification Report

Issue 1.0 06 February 2026

Expiry date 06 February 2031

TactiGuard VSI (Voice Stream Interceptor)

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

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

TactiGuard VSI (Voice Stream Interceptor) allows secure voice communication between different security levels.

TactiGuard VSI, Stock Number: 111500 and 111501, Version 3 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	06 February 2026
Expiry date	06 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 TactiGuard VSI Version 3 with Stock Numbers 111500 and 111501 for TPM version 1.2 and 2.0 respectively.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Saab Danmark A/S.

The main purpose of the TOE is to allow users to communicate through voice from a secure network to other networks at lower security levels. It is possible to have several different networks communicating using the same system.

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, four assumptions are made in the ST Public [12]. In order to counter five 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 Saab Danmark A/S.

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

Two security domains

TOE is normally used in a system solution with two security domains as shown in Figure 1 but can also be used for multiple (more than 2) number of security domains as shown in Figure 3.

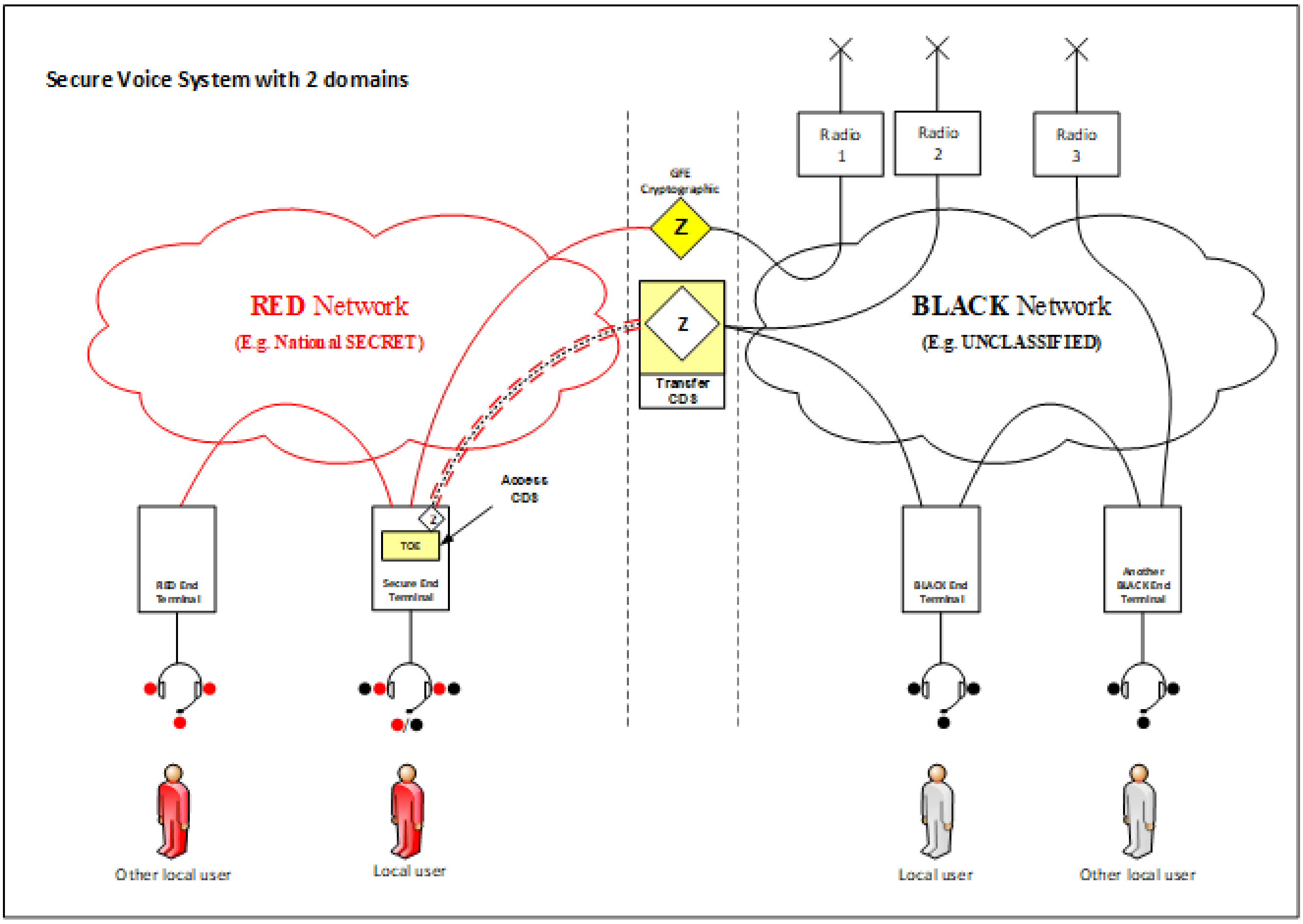

Figure 1 Voice System deployment with two security domains.

The shown communication lines are bi-directional

TOE makes sure that the Secure End Terminal can release voice streams, which only contains BLACK information (shown as dotted black line) and can be transported without loss of integrity (shown as dashed red line between Zs) over the classified network. The integrity check makes sure that no classified information in the classified network can be mixed with the BLACK (unclassified) voice stream. The user can make the selection between sending BLACK or RED information and gets an acknowledgement of the selection by a repeating non-secure warning tone while BLACK selection is made and the user is talking.

TOE is providing a security mechanism, which together with Virtual Private Network(s) (VPN(s)) is providing a secure release mechanism. In this way the Secure Voice System can interact with unclassified voice BLACK End Terminals or Radio (shown as example for Radio 2) outside the secure area. The unclassified network is not connected to the Internet.

For completeness the encryption of RED information has also been shown, where the Government Furnished Equipment (GFE) encryption is performed before it is transmitted via the radio (shown as example for Radio 1) and decrypted when receiving from the Radio into the RED Network.

The system solution is based on a “defence in depth” security strategy, where a number of security layers are applied. Each of the security layers are shown in Figure 2 both for incoming and outgoing data traffic.

TOE is controlling the suppression of RED incoming voice stream, such that while sending non-classified voice the possible pickup and cross talk of classified voice via the speaker to the microphone can be eliminated. The RED talking user (shown as ‘Other local user’ in Figure 1) will not be aware of the suppression.

Deployment

The following example deployment illustrates how the TOE can be used (see Figure 2), where the defence in depth approach also has been included.

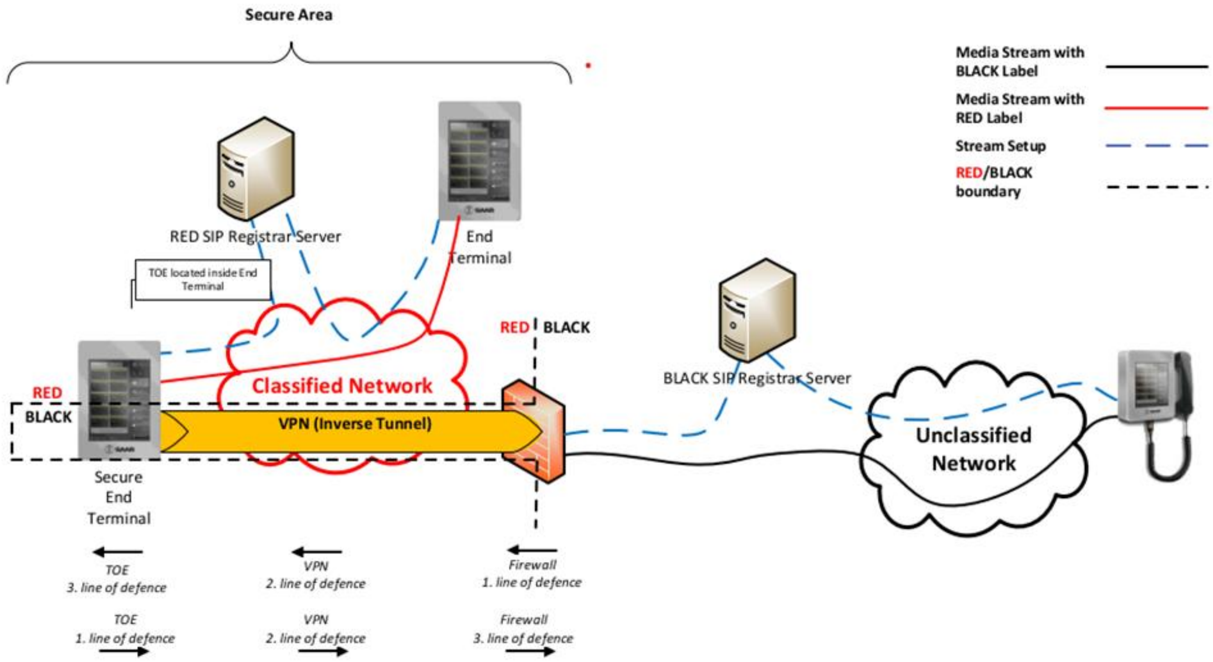

Figure 2 Example deployment of TOE in a secure voice system. TOE is located in the Secure End Terminal.

The following layers apply for incoming flow:

1. Only allowed protocol type can be sent from Unclassified Network to VPN.

2. Integrity of BLACK information is intact, because RED network equipment cannot modify data inside the inverse VPN tunnel.

3. Sanitation of incoming voice stream and setup is performed, such that defined protocol information is received.

The following layers apply for outgoing flow:

1. TOE performs separation between RED and BLACK information, such that only BLACK information is released to the inverse VPN tunnel.

2. VPN is preventing RED information from the Classified Network to mix with the Inverse Tunnel.

3. The Firewall is only allowing information from the VPN to be transmitted, such that no information from the classified network can be transmitted into the Unclassified Network.

4. Only allowed protocol type can be sent from VPN to Unclassified Network.

Figure 2 also shows that the communication line in Figure 1 actually is defined by the following:

- Voice Stream – the stream of IP packages containing voice information. The Real-time Transport Protocol (RTP) is used for the transportation of Voice Stream and Real-Time Transport Control Protocol (RTCP) for metadata transportation.

- Stream Setup – the communication required to setup the Voice Stream communication. The Session Initiation Protocol (SIP) and Internet Group Management Protocol (IGMP) are used for the Stream Setup.

The reason for dividing the communication is based on the required real time communication of Voice Stream.

The Stream Setup may require a so-called SIP Registrar such that end points can send Voice Stream according to the setup. Sanitization of Stream Setup is performed before being send to VPN inverse tunnel, which prevents it from being misused.

TOE stores audits in the underlying IT environment, where self-test, failures and success are stored for later retrieval.

Multiple security domains

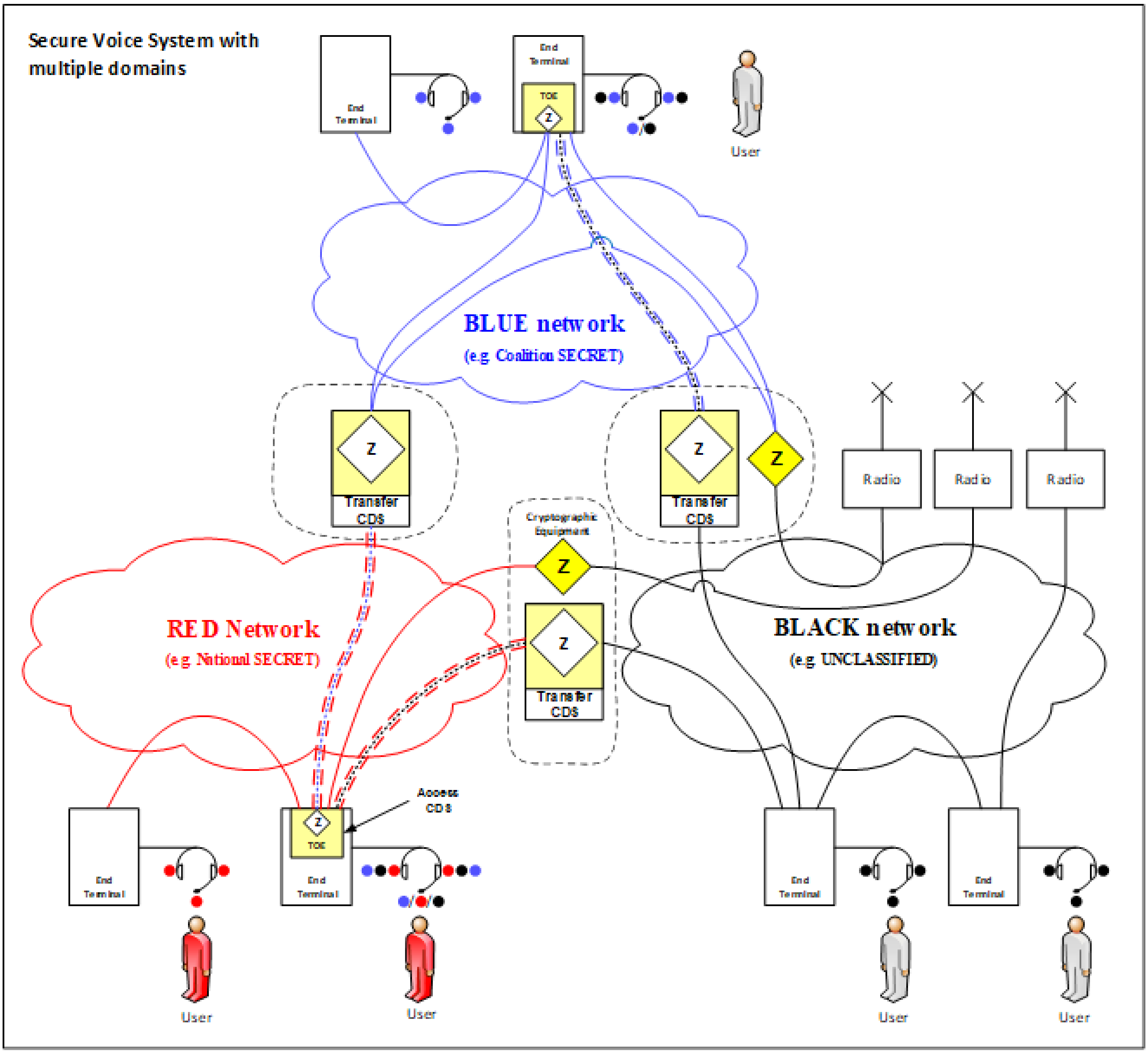

Figure 3 Voice System deployment with more than two security domains.

Support for additional classification levels (as example NATO classified information) is shown in Figure 3. This is performed in a similar way as BLACK information release. In the example, the additional domain is shown as BLUE information, which is transported without loss of integrity (shown as dashed red line between Zs) over the national classified network. The integrity check makes sure that no RED information in the national classified network can be mixed with the BLUE voice stream.

The user can make the selection between sending BLACK, BLUE or RED information. The user gets an acknowledgement of the selection by repeating non-secure warning tone respectively for BLUE or BLACK while BLUE or BLACK selection is made and the user is talking.

TOE is controlling the suppression of BLUE or RED incoming voice stream, such that while sending non-classified BLACK voice the possible pickup and cross talk of classified BLUE or RED voice via the speaker to the microphone can be eliminated. TOE does also support the suppression of RED voice stream, such that while sending BLUE voice the possible pickup and cross talk of classified RED voice to BLUE voice release can be eliminated.

2.1 Main security features:

TOE has been designed in such a way that it can be integrated into an overall system solution, where existing standard trusted products are used.

TOE makes it possible to provide the following important capabilities:

1. Secure Conferencing – multiple users can share a conference at the same classification level.

2. Release of classified and unclassified voice to another enclave with the correct classification level.

TOE located in RED domain provides the following security features, to support the above capabilities:

- TOE is a secure separation mechanism for voice streams, such that:
    - Transmission of BLACK streams to a VPN does not contain any RED or BLUE stream information.
    - Transmission of BLUE streams to VPN does not contain any RED stream information.
    - The user can listen to BLACK, BLUE and RED streams at the same time.

- TOE can minimise Cross talk of classified voice by suppression of incoming RED voice stream to the speaker while sending BLUE voice.

- TOE can minimise Cross talk of classified voice by suppression of incoming RED and BLUE voice stream to the speaker while sending BLACK voice.

Cross talk minimization is a feature, which can be enabled or disabled by a TOE configuration.

TOE located in BLUE domain provides the same security capabilities without the use of RED streams.

3 Assumptions and Clarification of Scope

3.1 Assumptions

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

- SECURE_IP
- SECURE_LOCATION
- SECURE_OS
- TRUSTED_VPN

For details on these assumptions, the reader is advised to look at chapter 4.3 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 four threats are countered by the TOE:

- TERMINAL_INTEGRITY
- WRONG_LABEL
- CORRUPT_STREAM
- CORRUPT_FORMAT

For details on these threats, the reader is advised to look at chapter 4.1.3 in the ST Lite [12]. The reader should also have a look at the description of the threat agents in chapter 4.1.2 in the ST Lite [12].

3.3 Threats Countered by the TOE environment

The threat T.NETWORK_INTEGRITY is countered by the environment. The first three threats in chapter 3.2 are also partially countered by the environment.

3.4 Organisational Security Policies

During the evaluation of the TOE the following four Organisational Security Policies have been considered:

- CIS_DEFINITION_POLICY
- CIS_PERSONNEL_POLICY
- VOICE_PROCEDURES_POLICY
- LABELLING_POLICY

All of the policies are compliant with applicable parts of Norwegian security policy [16] and NATO security policy [17]. The TOE Organizational Security Policies are detailed in Chapter 4.2 of the ST Lite [12].

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 27 October 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 24-28 November 2025.

5 Evaluated Configuration

The evaluated TOE, as described in chapters 1, 2 and Annex A, is SW only. The TOE is delivered as physical units with SW installed.

Installation of the TOE must be performed completely in accordance with the guidance documents [14], [15] 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.

5.1 Required non-TOE hardware/software/firmware

TOE requires the following non-TOE software:

- Common Criteria approved Linux Operating System (reflects the assumption A.SECURE_OS).
- IPsec tunnel (reflects the assumption A.TRUSTED_VPN).

TOE requires the following non-TOE hardware:

- Trusted Platform Module (TPM) either version 1.2 or version 2.0.

However, the Common Criteria approved Linux Operating System might have indirect requirements.

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 21 January 2026.

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 TactiGuard VSI 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 TactiGuard VSI 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], [15] included in the evaluated configuration.

One remark or possible improvement was given by the evaluation team:

Test (e) (“Running extreme load towards the TOE, such as excessive network traffic or high CPU usage”) was performed using DoS attacks with hping3. This resulted in the network interface of TOE shutting down, and voice communication was not working.

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
IGMP	Internet Group Management Protocol
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
ITSEF	IT Security Evaluation Facility under the Norwegian Certification Scheme
GFE	Government Furnished Equipment
PP	Protection Profile
RTCP	Real-Time Transport Control Protocol
RTP	Real-time Transport Protocol
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
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
VPN	Virtual Private Network

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, 08 January 2010.

[9] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, 02 July 2014.

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

[11] TactiGuard VSI - Security Target, Version 4, 02 December 2025

[12] TactiGuard VSI - Security Target Lite, Version 1, 02 December 2025

[13] Evaluation Technical Report for TactiGuard VSI, version 1.1, 21 January 2026.

[14] Installation Guidance for TactiGuard VSI (SVP-141), Revision 2, 03 December 2025

[15] Operational User Guidance for TactiGuard VSI (SVP-188), Revision 2, 04 December 2025

[16] Lov om nasjonal sikkerhet (Norwegian Security Act), LOV 2018-06-01 nr 24.

[17] C-M(2002)49, Security Within the North Atlantic Treaty Organisation (NATO), 17 June 2002.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

TactiGuard VSI, Stock Number: 111500 and 111501, Version 3

Refer to the manufacturer's documentation for additional information.

TOE Documentation

The supporting guidance documents evaluated were:

[a] Installation Guidance for TactiGuard VSI (SVP-141), Revision 2

[b] Operational User Guidance for TactiGuard VSI (SVP-188), Revision 2

TOE Configuration

The following two figures give the configurations/testbeds used for sample and selected subset testing of TOE, according to [43] “Test Plan”.

Testbed - Security function sample testing of TactiGuard VSI

The test bed for functional tests consists of two Virtual Machines connected through an SSH tunnel as seen in the Figure below:

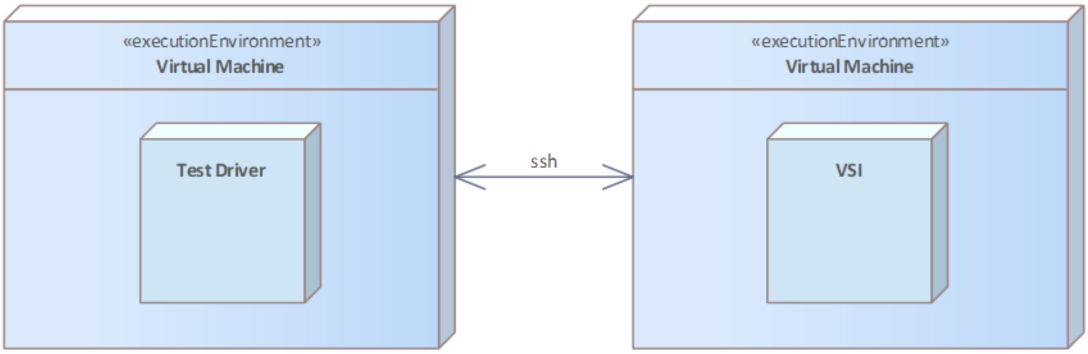

Figure 4 Test bed for functional tests

Testbed - Module sample testing of TactiGuard VSI

The test bed for module test consists of a Virtual Machine as seen in the Figure below:

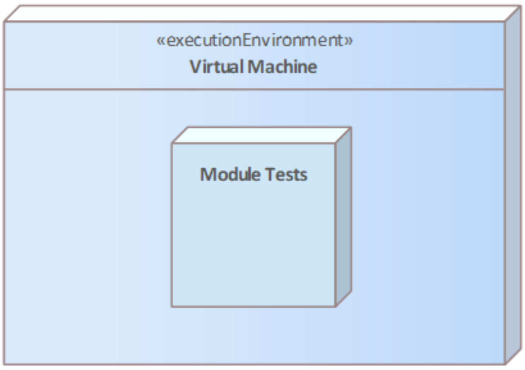

Figure 5 Test bed for module tests.

Testbed - Selected subset testing and penetration testing of TactiGuard VSI

NOTE: This test setup, which was used back in 2016 regarding the test activities for the previous evaluation, is now used with the following changes:

- The workstations stated in the figure as TSS3000 are replaced with workstations named as UT4440 (UT - User Terminals).
- The Red End Terminal is replaced with a Secure End Terminal.

The following figure presents a conceptual setup used for selected subset testing and penetration testing of TOE:

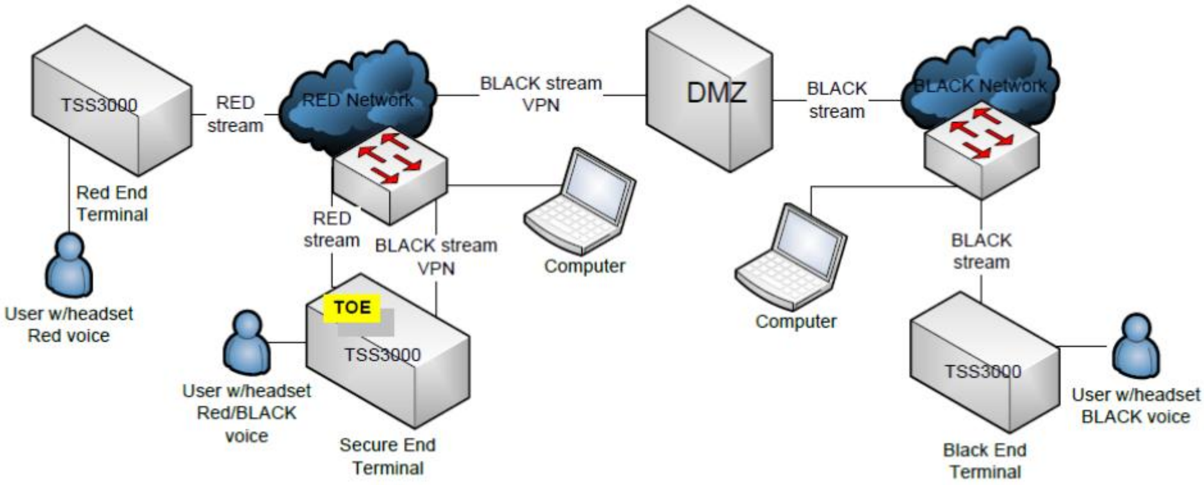

Figure 6 Test bed for selected subset tests and penetration tests.