SERTIT

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

# SERTIT-123 CR Certification Report

Issue 1.0 31 May 2024

Expiry date 31 May 2029

## MLS Voice Terminal 1.1.10

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

MLS Voice Terminal (MVT) provides a secure voice handling SW module inside an Operator Terminal (OCP) in an MLS Voice System (MVS).

MVT software version 1.1.10 has been evaluated under the terms of the Norwegian Certification Authority for IT Security [8] and has met the Common Criteria Part 3 (ISO/IEC 15408) [3] conformant components of Evaluation Assurance Level (EAL) 4 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 Public [10] with reference to the assumed operating environment specified by the ST Public [10]. 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 | 31 May 2024 |
| Expiry date | 31 May 2029 |

# 1 Executive Summary

Prospective consumers are advised to read this report in conjunction with the ST Public [10] which specifies the functional, environmental and assurance evaluation components.

The version of the product evaluated was MVT 1.1.10.

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

The TOE works together with the MLS Voice Guard (MVG) module of each Voice Guard to tunnel a lower classified voice stream from the OCP to a lower classified network via the Voice Guard. The TOE makes sure that the operator behind the OCP has clear information about the classification level of the network the microphone is connected to. The TOE also makes sure that the operator has information about whether any neighbouring OCPs have microphones connected to a lower classified network, and thereby can take measures when speaking classified information, e.g., speak lower.

The main purpose of the TOE is to provide the capabilities required to handle all voice presented at the OCP and to perform the required separation of voice data at different classification levels. The OCP is physically connected to the highest classified network. The TOE tunnels different classified voice data to corresponding networks via MVG in a secure way.

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, nine assumptions are made in the ST Public [10]. In order to counter seven threats as described in the ST Public [10], 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 [8], as well as the Common Criteria (CC) Part 3 [3] and the Common Evaluation Methodology (CEM) [4].

The evaluation was performed at the assurance level EAL 4 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 [9] was confirmed during the evaluation for the selected assurance level.

The basis for producing this Certification Report is the ST Public [10] and the ETR [11].

## 2 TOE overview and Security Policy

The TOE (MVT) is a building block in the operator terminal (OCP) of an MLS Voice System (MVS) that provides security related functions.The TOE is a part of the MLS Voice Platform (MVP) of the MVS.

The TOE is SW only, and is typically hosted on COTS hardware. The TOE runs on top of a separation kernel.

The MVP provides the capability to establish voice connections on different security levels from the same OCP. MVP is further divided into three parts:

(a) MLS Voice Terminal, this TOE (MVT)
(b) MLS Voice Guard (MVG)
(c) MLS Security Management (MSM)

The network with the highest security level is connected to a lower classified network. In effect,the MVP tunnels differently classified voice data from the OCP to networks of corresponding classifications in a secure way.

The users can receive audio in voice connections from one or more security levels simultaneously, while each user can transmit audio from the microphone according to security levels of the active voice connections. The OCP HMI displays the current security level(s) for the microphone audio, and the user must be trained to communicate information according to the displayed security level(s).

The MVG is the physical gateway between the internal (highest) security level and the external lower security level.

All audio streams are integrity protected according to their security level by the MVT (TOE).

There are specific MLS Voice Guards (MVGs) that handle the voice connections (VoIP) to the lower security levels. The MVG provides an automatic and controlled flow of information between two domains that may operate under different security policies. No information is allowed to pass from one of the domains to the other unless the Security Policy of the MVG explicitly allows it to pass.

The main security function of the OCP is to display the security levels that apply to the active (TX) connections

The OCP user has to look at the screen to be sure which information can be exchanged on the active voice connections. It is a manual and operational decision to only exchange information that is according to the displayed security levels (or any information with lower classification).

The OCP can have several active voice connections with different security levels, but the security levels displayed are the lowest security level within each security group (policy) that has active (TX) connections.

The transmitted and received audio for each individual MVT is sent to a centralised Voice Recorder.

The neighbour security status is used to inform the operator about possible low security microphone connections on the operator positions defined to be neighbours.

For use in an evaluated configuration, the MVT installation must be located in a physically secure environment to which only authorized users have access.

# 3 Assumptions and Clarification of Scope

## 3.1 Assumptions

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

- PHYSICAL
- TRAINING
- CLEARANCE
- MAN.AUTHORISED
- MVS.COM
- USAGE
- AUDIT
- MVT.ALARM
- HARDENING

For details on these assumptions, the reader is advised to look at chapter 3.2 in the ST Public [10].

## 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 ten threats are countered by the TOE:

- CONN.SEC.NON-SEC
- WRONG.SEC.IND
- ACOUSTIC.PICK-UP
- TEMPEST
- UNAUTHORISED.USE
- INFORMATION_LEAK
- OBJECT_TAMPERING

For details on these threats, the reader is advised to look at chapter 3.3.4 in the ST Public [10]. The reader should also have a look at the description of the threat agents in chapter 3.3.3 in the ST Public [10].

## 3.3 Threats Countered by the TOE environment

The following seven threats are met by the TOE environment

- AUDIT_FAILURE
- DELIVERY
- DOS
- IMPROPER_INST
- POOR_DESIGN
- POOR_IMPL
- UNATTENDED

For details on these threats, the reader is advised to look at chapter 3.3.2 in the ST Public [10].

## 3.4 Organisational Security Policies

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

- COUPLING
- ACCOUNTABILITY
- CRYPTOGRAPHY
- MINIMAL_POSTURE

All of the policies are compliant with applicable parts of Norwegian security policy [17] and NATO security policy [18]. The TOE Organizational Security Policies are detailed in Chapter 3.4 of the ST Public [10].

# 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 in 30 October 2023. No 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 tested the TOE Security Functionality Interfaces (TSFI) as described in the Design Specifications, and that the developer's 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 the TOE Security Functionality (TSF) subsystems against the TOE design and the security architecture description.

## 4.3 Evaluators' Tests

The evaluators performed independent testing of a subset of the TOE Security Functionality (TSF) 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 11-14 December 2023.

# 5 Evaluated Configuration

The evaluated TOE, as described in Chapters 1, 2 and Annex A, is SW only. The TOE is typically hosted on COTS hardware, and in protected VM compartments. The HW and VM platform is not part of the TOE.

Installation of the TOE must be performed completely in accordance with the guidance documents [12], [13], [14], [15], [16] provided by the developer. The TOE should be used in the operational environment as specified in the ST Public [10], as well as the guidance documents referenced in this chapter.

# 6 Evaluation Results

The evaluation addressed the requirements specified in the ST Public [10]. The ITSEF reported the results of this work in the ETR [11] 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 4 assurance package augmented with ALC_FLR.3.

| Assurance class | Assurance components | |
|---|---|---|
| Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.4 | Complete functional specification |
| | ADV_IMP.1 | Implementation representation of the TSF |
| | ADV_TDS.3 | Basic 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.4 | Problem tracking CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_DVS.1 | Identification of security measures |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_TAT.1 | Well-defined development tools |
| | 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.1 | Testing: basic design |
| | ATE_FUN.1 | Functional testing |

| | | |
|---|---|---|
| | ATE_IND.2 | Independent testing - sample |
| Vulnerability assessment | AVA_VAN.3 | Focused vulnerability analysis |

After due consideration of the ETR [11], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the certification team, SERTIT has determined that MVT 1.1.10 meets the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 4 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 MVT 1.1.10 should understand the specific scope of the certification by reading this report in conjunction with the ST Public [10]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST Public [10].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Chapters 1 and 2.

The TOE should be installed and operated in accordance with the supporting guidance documentation[12], [13], [14], [15], [16] included in the evaluated configuration.

# 8 Security Target

The complete Security Target [9]used for the evaluation performed is sanitised for the purpose of publishing. The Public version (Security Target Public [10]) is provided as a separate document. Sanitisation was performed according to the CCRA framework – ST sanitising for publication [5].

# 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 |
| 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 |
| MVG | MLS Voice Guard |
| MVP | MLS Voice Platform |
| MVS | MLS Voice System |
| MVT | MLS Voice Terminal |
| OCP | Operator Terminal |
| PP | Protection Profile |
| SERTIT | Norwegian Certification Authority for IT Security |
| 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 |
| TX | Transmit |
| VM | Virtual Machine |

# 10 References

[1] CCRA (2017), *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[2] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

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

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

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

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

[9] MLS Voice Terminal (MVT) Security Target, Ed7, 15 December 2023

[10] Security Target Public,

[11] Evaluation Technical Report for the Evaluation of MVT 1.1.10, version 1.1, 12 February 2024.

[12] Operator Control Position Operator Manual, Ed 2023-10-26

[13] MLS Security Management User Manual, Ed1.1.2

[14] Site Management Application User Manual, Ed9.1.3

[15] Operator Control Position Technical Manual, Ed9.1.1

[16] Version Delivery Description (VDD), Ed1.1.10

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

[18] 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:

MVT 1.1.10 software

The TOE is typically hosted on COTS hardware, and in protected VM compartments.

Refer to the manufacturer’s documentation for additional information.

## TOE Documentation

The supporting guidance documents evaluated were:

[a] Operator Control Position Operator Manual, Ed 2023-10-26

[b] MLS Security Management User Manual, Ed1.1.2

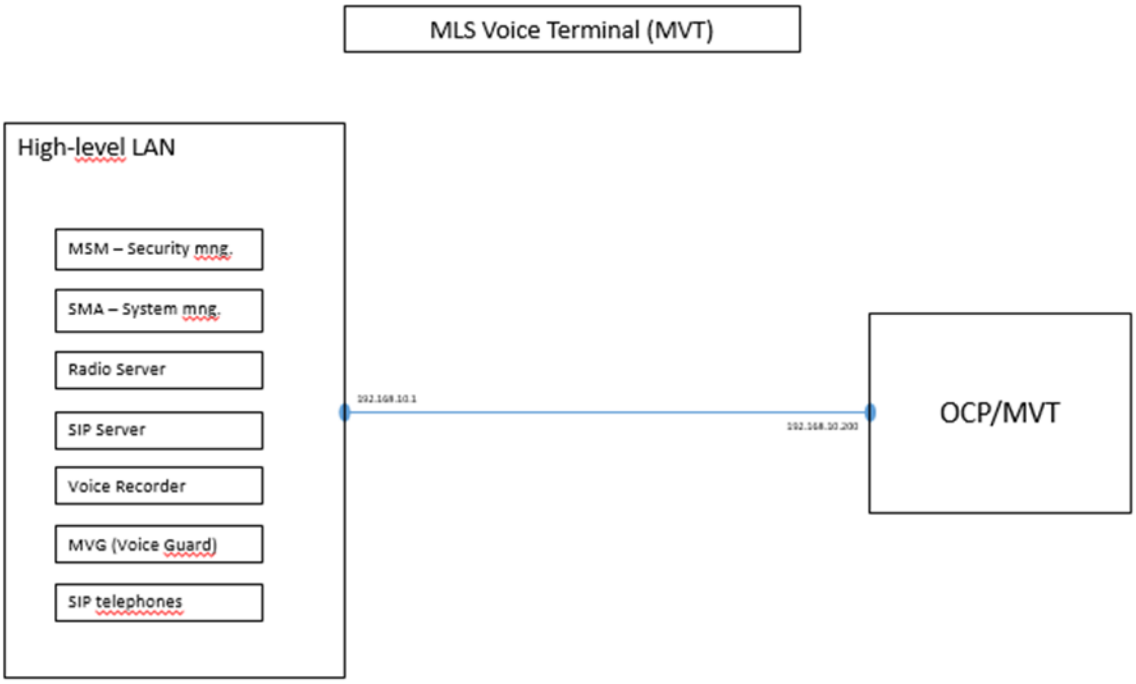
[c] Site Management Application User Manual, Ed9.1.3

[d] Operator Control Position Technical Manual, Ed9.1.1

[e] Version Delivery Description (VDD), Ed1.1.10

## TOE Configuration

The following configuration was used for testing:


MLS Voice Terminal (MVT)
High-level LAN
MSM – Security mng.
SMA – System mng.
Radio Server
SIP Server
Voice Recorder
MVG (Voice Guard)
SIP telephones
192.168.10.1
192.168.10.200
OCP/MVT