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

SERTIT-072 CR Certification Report

Issue 1.0 21.06.2017

Voice Stream Interceptor (VSI) Stock no. SV000071 version 1

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009E VERSION 1.1 01.07.2015

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 Common Criteria Recognition Arrangement logo printed on this Certification Report and the Certificate indicates that this certification is recognised under the terms of the CCRA July 2 2014. Mutual Recognition under the CCRA is limited to EAL 2 augmented 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.

The SOGIS logo printed on this Certification Report and the Certificate indicates that this certification is recognised under the terms of the SOGIS MRA January 2010, v 3.0. Mutual Recognition under the SOGIS MRA is limited to EAL 4 CC part 3 components.

Contents

1 Certification Statement 4

2 Abbreviations 5

3 References 7

4 Executive Summary 8
4.1 Introduction 8
4.2 Evaluated Product 8
4.3 TOE scope 9
4.4 Protection Profile Conformance 9
4.5 Assurance Level 9
4.6 Security Policy 10
4.7 Security Claims 11
4.8 Threats Countered by the TOE and the TOE environment 11
4.9 Threats and Attacks not Countered 11
4.10 Environmental Assumptions and Dependencies 11
4.11 Security Objectives for the TOE 12
4.12 Operational Environment Security Objectives 12
4.13 Security Functional Components 13
4.14 Security Function Policy 13
4.15 Evaluation Conduct 14
4.16 General Points 14

5 Evaluation Findings 16
5.1 Introduction 17
5.2 Delivery 17
5.3 Installation and Guidance Documentation 17
5.4 Misuse 17
5.5 Vulnerability Analysis 17
5.6 Developer's Tests 18
5.7 Evaluators' Tests 18

6 Evaluation Outcome 21
6.1 Certification Result 21
6.2 Recommendations 21

Annex A: Evaluated Configuration 22
TOE Identification 22
TOE Documentation 22
TOE Configuration 22

1 Certification Statement

Voice Stream Interceptor (VSI) is an Access Cross Domain Solution (CDS) in a VoSIP solution, where voice information with different classification levels can be handled. This is achieved by the means of Secure Voice Labelling. The secure voice labelling 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.

Voice Stream Interceptor (VSI) Stock no. SV000071 version 1 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 [4] (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 5 augmented with Systematic Flaw Remediation ALC_FLR.3 for the specified Common Criteria Part 2 [3] (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Certifier	Lars Borgos Lars Borgos
Quality Assurance	Arne H. Rage Arne H. Rage
Approved	Kristian S. Bae Elin Haugan Head of SERTIT
Date approved	21.06.2017

2 Abbreviations

Access CDS	General category of IT products like keyboard, video and mouse (KVM), switch etc.
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCEB	Combined Communications Electronics Board
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CDS	Access Cross Domain Solution
CEM	Common Methodology for Information Technology Security Evaluation
CIS	Communication and Information Systems
C2	Command and Control
DMZ	De-Militarized Zone
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
LSE	Local Security Environment – A controlled Access Facility
NDLO	Norwegian Defence Logistics Organization Naval System
NSA	National Security Authority
OSP	Organizational Security Policy
SERTIT	Norwegian Certification Authority for IT Security
SIP	Session Initiation Protocol
SOGIS MRA	SOGIS Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

VoSIP	Voice over Secure IP
VPN	Virtual Private Network
VSI	SAAB product name for the TOE categorized as an Access CDS

3 References

[1] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security*, Version July 2, 2014.

[2] CCRA (2012), *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] CCRA (2012), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] CCRA (2012), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] CCRA (2012), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2012-09-004, Version 3.1 R4, September 2012.

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

[7] NTT Security (Norway) AS (2017), *Evaluation Technical Report: Common Criteria EAL Evaluation of Voice Stream Interceptor (VSI)*, Stock Number: SV000071, Version: 1, Issue: 1.1, 20.02.2017.

[8] Saab Danmark AS (2016), *Operational User Guide for Voice Stream Interceptor*, SV000038 Ed2, 13.10.2016.

[9] Saab Danmark AS (2016), *Installation Guidance for Voice Stream Interceptor*, SV000037 Ed4, 24.11.2016.

[10] Saab Danmark AS (2016), *Security Target Lite for Voice Stream Interceptor (VSI) Product*, SV000073, Revision 1, 08.12.2016.

[11] Saab Danmark AS (2016), *Security Target for Voice Stream Interceptor (VSI) Product*, SV000008, Revision 12, 08.11.2016.

[12] SERTIT (2013), *The Norwegian Certification Scheme*, SD001E, Version 9.0, 2 April 2013.

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

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Voice Stream Interceptor (VSI) Stock no. SV000071 version 1 to the Sponsor, NDLO, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

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

4.2 Evaluated Product

The version of the product evaluated was Voice Stream Interceptor (VSI) Stock no. SV000071 version 1.

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

1) The Voice Stream Interceptor Product (the TOE) is categorized as an Access Cross Domain Solution (CDS) in a VoSIP solution, where voice information with different classification levels can be handled. This is achieved by the means of Secure Voice Labelling. The secure voice labelling 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.
2) The system solution is based on a "defence in depth" security strategy, where a number of security layers are applied as described in Security Target [10] section 1.4.
3) TOE makes sure that the Secure End Terminal can release voice streams, which only contains BLACK information and can be transported without loss of integrity 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.
4) TOE is providing a security mechanism, which together with a DMZ is providing a secure release mechanism. In this way the voice system can interact with unclassified voice End Terminals outside the secure area. The unclassified network is not connected to the Internet.
5) TOE is a secure separation mechanism for voice streams.
6) TOE is also 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 will be eliminated.

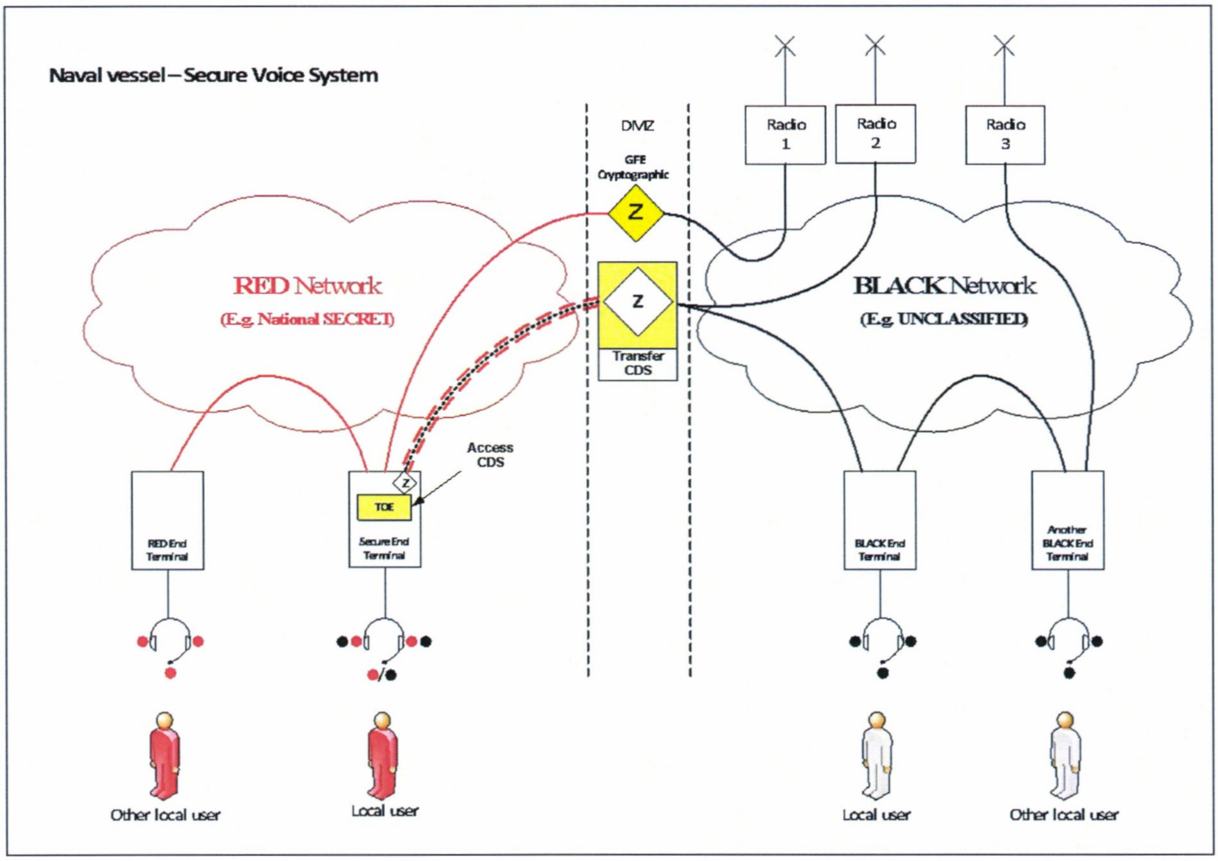

Figure 1: Voice System deployment with two security domains. The shown communication lines are bidirectional.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

Voice Stream Interceptor (VSI)

Stock no. SV000071 version 1

4.4 Protection Profile Conformance

The Security Target [10] did not claim conformance to any registered Protection Profile.

4.5 Assurance Level

The Security Target [10] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 5 augmented with Systematic Flaw Remediation ALC_FLR.3 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [1].

4.6 Security Policy

The operational environment of the TOE is Communications and Information Systems (CIS). CIS are an essential part of military operations and provide commanders at all levels with the means to exercise Command and Control (C2) and disseminate classified information. CIS must be accredited specifically to handle classified information by a National Security Authority (NSA). Operating authority who is handling accredited CIS classified information system must issue instructions for processing, handling and accounting for classified information.

CIS handling classified information shall use a trusted release mechanism for release of unclassified or BLACK Voice Stream information. The trusted release mechanism provided by the TOE shall prevent unintended release of Classified or RED Voice Stream information.

The main functionality of the TOE is to implement the policy for labelling in an automated way. The TOE documentation supports operating authorities with CIS handling classified information to be accredited, where BLACK Voice Stream information flows by tunnelling. The tunnelling provides a means to interconnect the TOE and the unclassified network using the classified network as communication bearer service.

- P.CIS_DEFINITION_POLICY The TOE, classified and unclassified network are according to AC/322-D/0030 defined as one CIS and under the control of one and the same CIS operating authority.
- P.CIS_PERSONNEL_POLICY CIS operators are military personnel with authorised access to the CIS based on their security clearance.
- P.CIS_INTERCONNECTION_POLICY Interconnection from both CIS classified and unclassified network to other CIS are known and controlled according to AC/322-D/0030 by the CIS operating authority.
- P.VOICE_PROCEDURES_POLICY The TOE shall, by an appropriate release mechanism, pass speech traffic as securely as possible consistent with accuracy, speed and the needs of command and control (C2) according to the Combined Communications Electronics Board (CCEB) in the Allied Communications Publication (ACP) 125 "Radiotelephone Procedures".
- P.LABELLING_POLICY The TOE shall implement and comply with the labelling policy appropriate for handling classified information. This policy defines the
    - Labelling: the trusted indication of the classification level of the voice stream.
    - Security rules: the set of rules for the circumstances under which information will be allowed for declassification. In [SFP.BLACK_STREAM] this policy is fully defined, see section 6.1.2.1 and 6.1.3.1 in Security Target [10].

4.7 Security Claims

The Security Target [10] fully specifies the TOE's security objectives, the threats and OSP's which these objectives meet and security functional components and security functions to elaborate the objectives. The SFR's are taken from CC Part 2 [3]; use of this standard facilitates comparison with other evaluated products. No extended components are defined.

4.8 Threats Countered by the TOE and the TOE environment

- T.TERMINAL_INTEGRITY: The Secure End Terminal (TA.TSS_APPLICATION) may mix Non-Classified and Classified Voice Stream (AS.RED_VOICE), which could violate the security rules.
- T.NETWORK_INTEGRITY: An internal user or resource (TA.INTERNAL) may corrupt the Voice Stream, such that Classified Voice Stream (AS.RED_VOICE) could be released to unclassified network.
- T.WRONG_LABEL: The user (TA.USER) may select a wrong classification of a Voice Stream, which could lead to a violation of the security rules for Classified Voice Stream (AS.RED_VOICE).
- T.CORRUPT_STREAM: An external user (TA.EXTERNAL) could send a corrupt incoming voice stream, so that a Secure End Terminal integrity failure could lead to a violation of the security rules for Classified Voice Stream (AS.RED_VOICE).
- T.SETUP: Resources in the DMZ might be used by an external user (TA.EXTERNAL) to perform a tampering setup such that a violation of the security rules for Classified Voice Stream (AS.RED_VOICE) may occur.
- T.CORRUPT_FORMAT: An external user (TA.EXTERNAL) might corrupt the stream setup, so that a Secure End Terminal integrity failure could lead to a violation of the security rules for Classified Voice Stream (AS.RED_VOICE).

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

- A.SECURE_IP: Secure End Terminal containing TOE is connected to a Secure IP network, which means that measures for the secure transmission are fulfilled.
- A.SECURE_LOCATION: TOE is located in a secure area.
- A.SECURE_OS: TOE is executing on a Common Criteria evaluated OS with Assurance Level 3 or higher and has been configured with a hardening setup.

- A.TRUSTED_VPN[1]: TOE has a VPN connection to the DMZ, to prevent access to classified voice stream (AS.RED_VOICE).

4.11 Security Objectives for the TOE

- OT.SANITY_CHECK: The TOE shall perform sanity check of Requested BLACK Voice Stream Header, Requested BLACK Stream Setup, Incoming BLACK Voice Stream Header and Incoming BLACK Stream Setup.
- OT.SELECTOR: The TOE shall support the user in the reliable BLACK TALK operation.
- The TOE shall issue a non-secure warning tone when receiving the Requested BLACK Voice Stream and the selector is in position BLACK TALK.
- The non-secure warning tone is repeated periodically, while receiving Requested BLACK Voice Stream and the selector is in position BLACK TALK.
- OT.SUBSTITUTION: The TOE shall provide Outgoing BLACK Voice Stream, where the Voice content of Requested BLACK Voice Stream is substituted with the incoming microphone stream.
- Substitution with incoming microphone stream is only made, when selector is BLACK TALK. Otherwise, the outgoing Voice Stream is blocked.
- OT.SEND: The TOE shall send BLACK Voice Stream and Setup through the trusted release (OE.TRUSTED_RELEASE).
- OT.LOG: The TOE shall store the failure of the substitution, integrity check and sanity check in a log.
- OT.ROBUST: The TOE shall be robust, such that internal TOE errors are handled appropriately.
- OT.SUPPRESS: The TOE can prevent acoustic feedback from the local speaker of the incoming RED Voice Stream when selector is BLACK TALK and receiving Requested BLACK Voice Stream.

4.12 Operational Environment Security Objectives

- OE.SECURE_IP: The communication infrastructure used by the TOE shall be a Secure IP.
- OE.SECURE_LOCATION: The TOE shall be installed within controlled access facilities (LSE).
- OE.ENVIRONMENTAL: The TOE shall operate within the manufacturer's environmental specification.
- OE.ACOUSTIC_FEEDBACK: The risk of acoustic feedback in the environment shall be addressed by operational procedures.

[1] Note: A threat could be stated instead of the assumption. However, the trusted VPN is a very generic security functionality and will be available in the IT Environment. Therefore the threat has not been stated and instead an assumption has been made.

- OE.INSTRUCTED_USERS: Trusted direct users are assigned, instructed and shall act as such in using equipment where the TOE is located.
- OE.INSTRUCTED_ADMIN: Trusted direct users are assigned, instructed and shall act as such to manage the TOE.
- OE.EVALUATED_OS: The operating system the TOE makes use of shall be evaluated OS. SFR FPT_STM.1, FMT_MSA.1 and FMT_SMR.1 shall be part of the OS due to dependencies between TOE SFRs.
- OE.LOG_ACCESS: The IT Environment shall allow only the administrator (S.ADMIN) read access to the Log.
- OE.READ_LOG: The S.ADMIN shall be able to read the TOE Log.
- OE.TRUSTED_RELEASE: A trusted release security mechanism between the classified network within the LSE and the external system shall be used for the release of Unclassified Voice Streams. The trusted Voice Stream Labelling of the TOE is utilised by the trusted release security mechanism.
- OE.TRUSTED_REGISTRAR: A trusted release security mechanism between the classified network within the LSE and the external system shall provide a trusted SIP Registrar.
- OE.PREVENT_ACCESS: A Trusted VPN between the TOE and DMZ shall be used. The trusted VPN act as an inverse tunnel, such that uncontrolled access to the classified network is prevented. In this way, the Classified Network is only used as a pure transport of voice.

4.13 Security Functional Components

- FAU_GEN.1 Audit data generation
- FDP_IFC.1(1) Subset information flow control
- FDP_IFC.1(2) Subset information flow control
- FDP_IFC.1(3) Subset information flow control
- FDP_IFF.1(1) Simple security attributes
- FDP_IFF.1(2) Simple security attributes
- FDP_IFF.1(3) Simple security attributes
- FMT_MSA.3 Static attribute initialisation
- FPT_FLS.1 Failure with preservation of secure state
- FPT_TST.1 TSF testing
- FTP_TRP.1 Trusted path

The full description of the SFRs can be found in the Security Target [10], section 6.1.

4.14 Security Function Policy

- Information flow control policy FDP_IFC.1.1(1) The TSF shall enforce the [SFP.BLACK_STREAM] on [the subjects S.TSS and S.DMZ via OE.PREVENT_ACCESS, Send operation, on the information O.BLACK_VOICE_STREAM].

- FDP_IFC.1.1(2) The TSF shall enforce the [SFP.BLACK_SETUP] on [the subjects S.TSS and S.DMZ via OE.PREVENT_ACCESS, Send operation, on the information O.STREAM_SETUP].
- FDP_IFC.1.1(3) The TSF shall enforce the [SFP.RED_STREAM] on [the subjects S.TSS, Receive operation, on the information O.RED_VOICE_STREAM].

4.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA) and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA). The evaluation was conducted in accordance with the terms of the Arrangement and the Agreement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [10], which prospective consumers are advised to read. To ensure that the Security Target [11] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [5].

SERTIT monitored the evaluation which was carried out by the NTT Security (Norway) AS (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR) [6] to SERTIT on the 20.02.2017. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the Security Target [10] with reference to the assumed operating environment specified by the Security Target [10]. The evaluated configuration was that specified in 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.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 5 assurance package augmented with Systematic Flaw Remediation 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_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_FLR.3	Systematic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
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

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target [10]. The results of this work were reported in the ETR [6] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

Delivery of the TOE to the customer is done using two different channels of transport. The TOE itself is delivered on a USB drive via physical transport as appropriate. The calculated SHA256 hash, located at working/vsi/vsi.sha256, is delivered through a different type of transport. Any electronic type of transport can be used as appropriate.

On receipt of the TOE, the administrator must make sure the evaluated version has been supplied and to check that the security of the TOE has not been compromised in delivery by verifying the integrity of the USB driver against the SHA256 hash as described in the Installation Guidance [9].

5.3 Installation and Guidance Documentation

The TOE can be integrated into an overall system solution where existing standard trusted products are used. Besides, cross talk minimization is a feature, which can be enabled or disabled by a TOE configuration.

The preparative procedures and installation of the TOE should be done as described in the Installation Guidance [9].

The TOE should be used as described in the Operational User Guide [8].

5.4 Misuse

The TOE is a software component designed to be an integrated part of a CIS.

Administrators should follow the Installation Guidance [9] for the TOE in order to ensure that the TOE is installed and configured in a secure manner.

The TOE should be used as described in the Operational User Guide [8].

5.5 Vulnerability Analysis

The evaluator's team did not find any specific area of concern when examining the Functional Specification, Security Architecture, Subsystem Design and Module Design. The evaluator's team searched for known vulnerabilities in public available sources, and did not find any public available information identifying and describing possible attack scenarios for the TOE type. The evaluator's team used the search engine Google on the 18.10.2016 without finding any issues regarding 'access cross domain solution vulnerabilities'.

The Evaluators' vulnerability analysis was successfully completed as the methodical vulnerability analysis has met the EAL5 evaluation criteria of AVA_VAN.4. This also includes all threats described in the Security Target [10], section 3.1.3.

The evaluator's team developed and conducted penetration tests based on the developer's vulnerability analysis and the evaluator's independent vulnerability analysis.

5.6 Developer's Tests

The Developer's tests were performed as a black box test that tested all public interfaces. Tests were performed at different abstraction levels like TSF Interfaces, TSF, Subsystems and Modules by testing security functions and modules.

The evaluators' assessments of the developers' tests shows that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements. The testing performed on the TOE by both the developer and evaluator showed that the EAL 5 assurance components requirements are fulfilled.

Developer testing VSI	**Test amount**
Security Function testing	54
Service Executor Subsystem Module testing	81
Integrity Check Subsystem Module testing	10
Audio Control Subsystem Module testing	22
Tunnel Control Subsystem Module testing	132
Stream Silencer Subsystem Module testing	34
Sum	333

Table 1: Amount of the developer testing performed

5.7 Evaluators' Tests

The selected test strategy was based on an assessment of the identified threat agents and the assets protected by the TOE.

The evaluation team decided to perform the testing on modules for all 5 TSF subsystems for sample testing:

- Service Executor subsystem
- Integrity Check subsystem
- Audio Control subsystem
- Tunnel Control subsystem
- Stream Silencer subsystem

The evaluation team decided to perform the testing on all 12 TSFIs for sample testing:

1. BLACK Voice Stream
2. BLACK Stream Setup
3. Encapsulation Tunnel
4. Microphone
5. Speaker
6. Control
7. Configuration
8. Incoming RED Voice Stream
9. RED Voice Stream
10. Log
11. TPM (Trusted Platform Module)
12. Service

The evaluation team decided to perform the testing on all TSFIs, on all TSF subsystems, and the TSF modules by means of:

- Security Function testing
- Module testing

The evaluator's team used the test coverage and the depth of testing analysis as a basis for the sample testing selection. The amount of the sample testing selection constitutes about 30 % of the total developer tests on all TSFIs, all TSF subsystems, and the TSF modules, which the evaluator's team considered to sufficient since sample testing normally should constitute 20-30 % of the total developer module interface tests. The testing was performed at the Developers facility at 09.11.2016.

Developer testing VSI	**Test amount**
Security Function testing	17
Service Executor Subsystem Module testing	24
Integrity Check Subsystem Module testing	3
Audio Control Subsystem Module testing	7
Tunnel Control Subsystem Module testing	39
Stream Silencer Subsystem Module testing	10
Sum	100

Table 2: Amount of the evaluators sample testing performed.

The evaluator's team focused the devised testing on areas or issues not explicit handled by the developer testing. The testing was comprised of the following TSFIs: Encapsulation Tunnel, Microphone, Speaker, Control, Log and Service. The test configuration used for devised testing of VSI was as described in Figure 4, except the Computer which was used for the penetration testing.

All 100 scenarios from the sample testing and all the scenarios from the devised testing have been successfully performed with the expected results.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [6], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Voice Stream Interceptor (VSI) Stock no. SV000071 version 1 meets the Common Criteria Part 3 [4] conformant components of Evaluation Assurance Level EAL 5 augmented with Systematic Flaw Remediation ALC_FLR.3 for the specified Common Criteria Part 2 [3] conformant functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Voice Stream Interceptor (VSI) Stock no. SV000071 version 1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [10]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target [10].

Only the evaluated TOE configuration should be installed [9]. This is specified in Annex A with further relevant information given above in section 4.3 TOE scope and section 5 Evaluation Findings.

The TOE should be used in accordance with the supporting guidance documentation [8] included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE is identified as:

Name:	Voice Stream Interceptor
Stock Number:	SV000071
Version:	1

TOE Documentation

The supporting guidance documents evaluated were:

[a] Saab Danmark (2016), *Installation Guidance for Voice Stream Interceptor*, SV000037 Ed4, 24.11.2016.

[b] Saab Danmark (2016), *Operational User Guide for Voice Stream Interceptor*, SV000038 Ed2, 13.10.2016.

[c] Saab Danmark (2016), *Security Target for Voice Stream Interceptor (VSI) Product*, SV000008, Revision 12, 08.11.2016.

Further discussion of the supporting guidance material is given in Section 5.3 Installation and Guidance Documentation.

TOE Configuration

The following configuration was used for testing:

Voice Stream Interceptor, which is purely software and can be installed on several physical devices as long as the following non-TOE software requirements are valid:

- Common Criteria approved Operating System, with Evaluated Assurance Level 3 or higher and configured with a hardening setup. A Common Criteria approved Linux Operating System was used in the Evaluated configuration.
- IPsec tunnel, whereby VSI has a VPN connection to the DMZ to prevent access to classified voice stream.

The used test environments were according to the testbeds as described in figures 2 – 4.

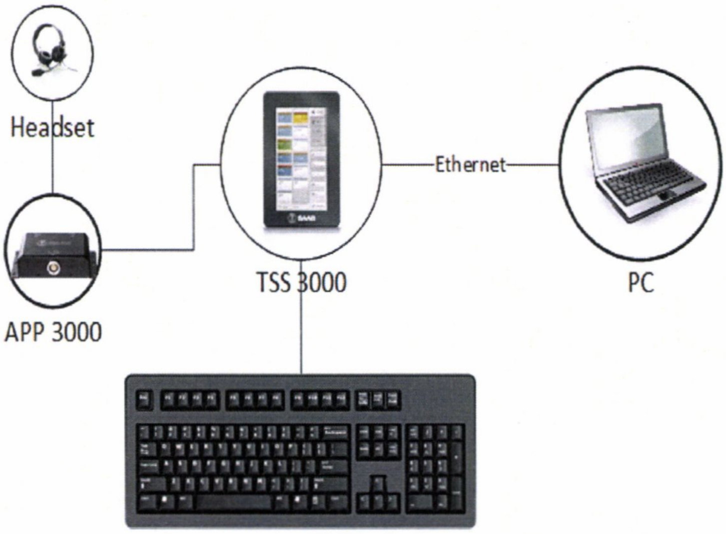

Figure 2: Testbed for Security functional sample testing

Testbed for security functional sample testing consists of a Secure End Terminal with attached APP3000 and a PC with test software connected.

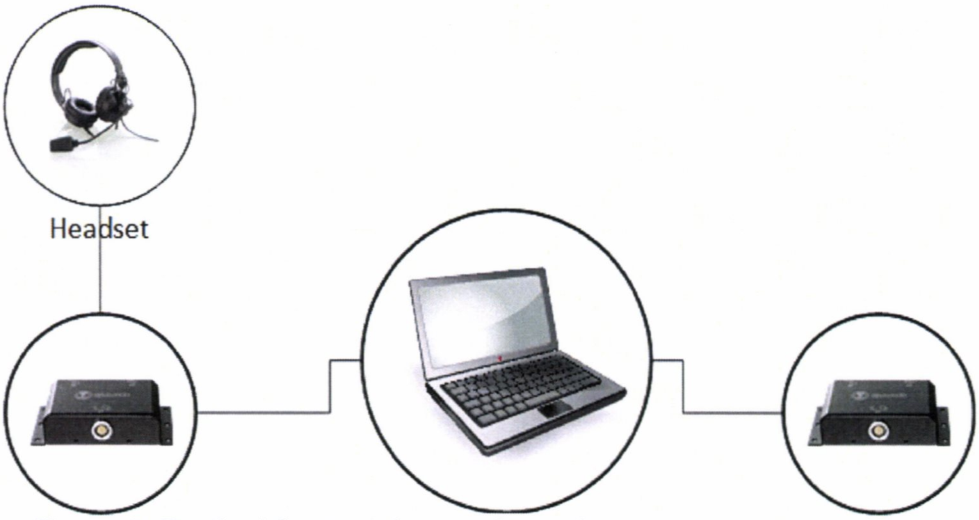

Figure 3: Testbed for module sample testing

Testbed for module sample testing consists of a PC installed with VMware and test software with attached APP3000 and headset.

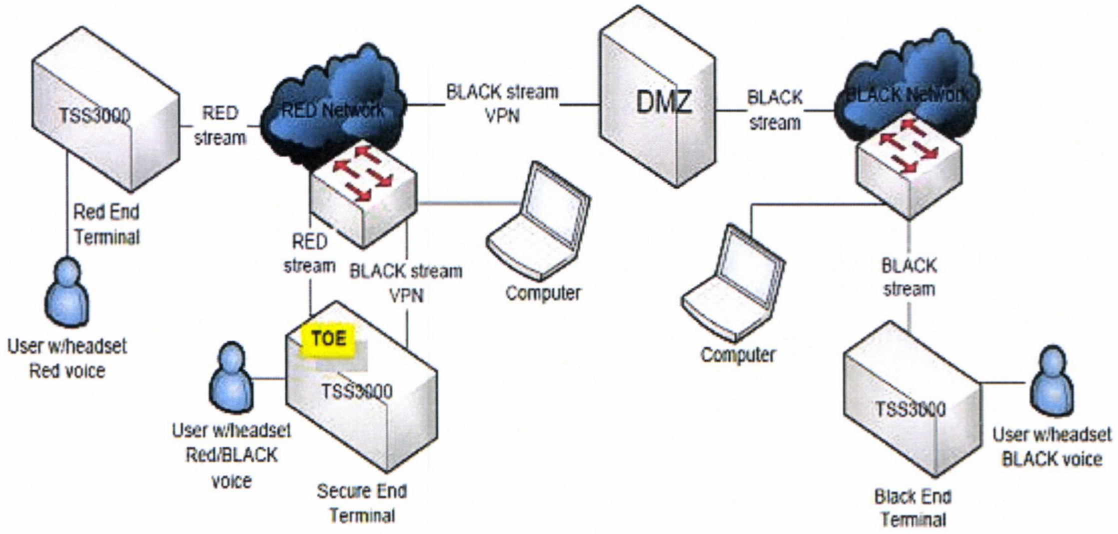

Figure 4: Testbed for devised and penetration tests

Testbed for devised testing consists of the Saab operational test environment, and has not a Computer connected.

Testbed for penetration testing consists of the Saab operational test environment and a Computer with test software connected.