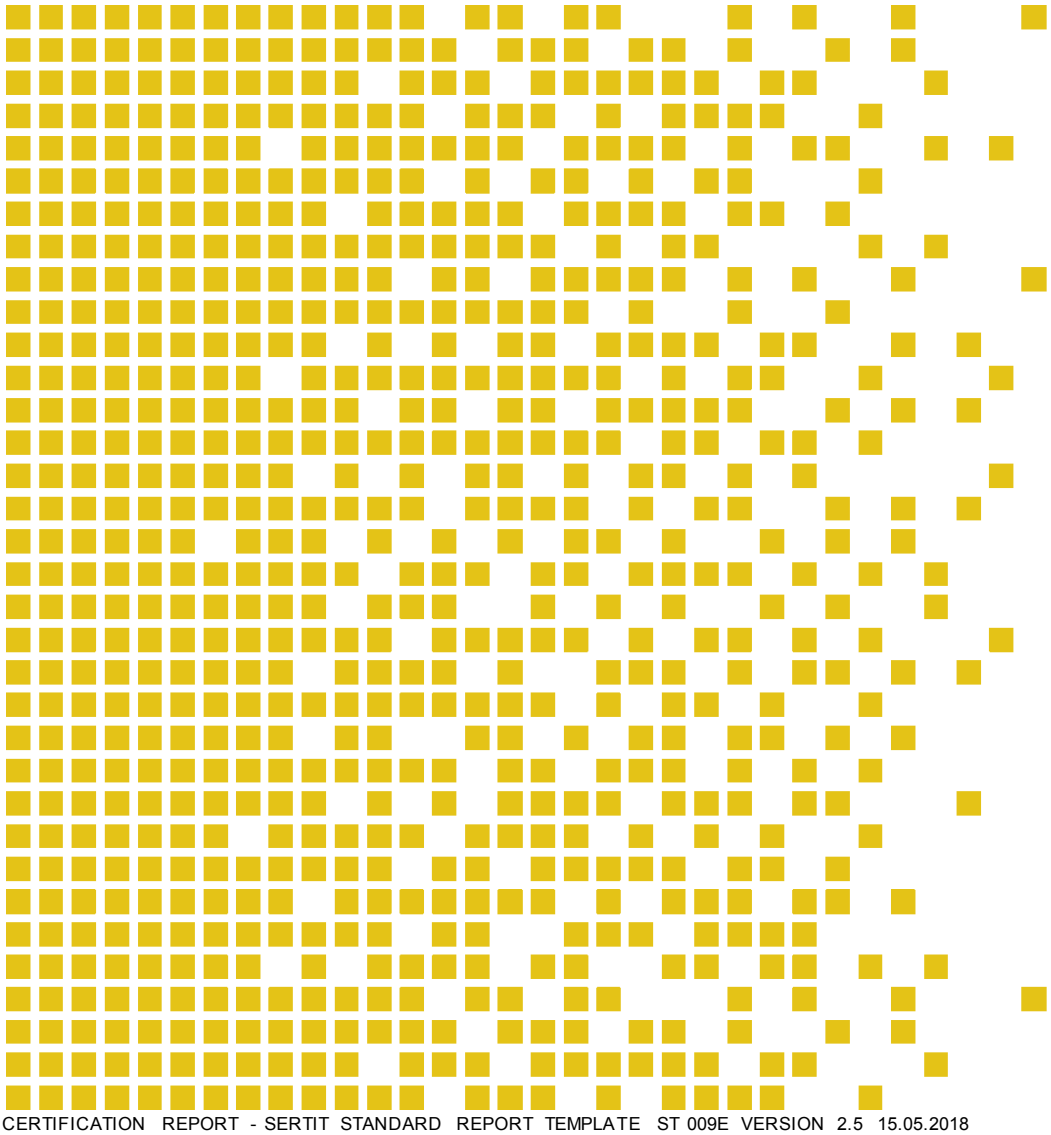
SERTIT
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*
SERTIT er en del av Nasjonal sikkerhetsmyndighet *SERTIT is a part of Norwegian National Security Authority*

SERTIT-101 CR Certification Report

Issue 1.0 15 July 2019

Expiry date 15 July 2024

Operator Terminal Adapter (OTA): OTA hardware: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B; OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5



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

This page is intentionally left blank.

1 Certification Statement

Thales Norway AS Operator Terminal Adapter (OTA) is part of the Voice Communication Systems (VCS) used in operation sites. The main purpose of the OTA is to provide capabilities required to handle all voice presented at the Operator Controller Position (OCP) and to perform the required red/black separation of voice and data.

Operator Terminal Adapter (OTA) with

OTA Hardware versions: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B;

OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5

has been evaluated under the terms of the Norwegian Certification Authority 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 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, SERTIT
Date approved	15 July 2019
Expiry date	15 July 2024

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCI	Controlled Cryptographic Item
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045)
DSP	Digital Signal Processor
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
LED	Light Emitting Diodes
LOL	Loudspeaker and Lamps
MFT	Multifunction Terminal
OCP	Operator Controller Position
OTA	Operator Terminal Adapter
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SMA	Site Management Application
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
VCS	Voice Communication Systems

3 References

[1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

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

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

[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] Thales Norway AS (2019), *Security Target for OTA*, Thales Norway AS, 3AQ 24863 AAAA 377 EN, version 6.2.9, 25 Mar 2019.

[9] System Sikkerhet AS (2019), *Evaluation Technical Report (ETR) – Common Criteria EAL5 Evaluation of OTA*, Issue 1.1, 2019-06-24.

[10] Thales Norway AS (2016), *Guidance to Security Officer*, AL1V-03-00682-D, Edition D, 13 June 2016.

[11] Thales Norway AS (2018), *Security Design – part 1*, 3AQ 24863 AAAA DEZZA, Edition 6.2.4, 8 August 2018.

[12] Thales Norway AS (2017), *Security Design – part 2*, 3AQ 24863 AAAA DEZZA, Edition 6.2.2, 21 November 2017.

[13] Thales Norway AS (2018), *Technical Manual*, 3AQ 12889 ABAC EO, Edition 8, 29 January 2018.

[14] Thales Norway AS (2015), *VCF Operator Position Manual*, AL1V-14-00453-G VOL-01C, Edition G, 15 October 2015.

[15] NATO (2008), NATO Security Committee – *Directive on Physical Security* AC/35-D/2001-REV2, 7 January 2008.

[16] Crypto security regulations (2018), *Forskrift om kryptosikkerhet*, FOR-2018-12-20-2055, Ministry of Justice- and Public Security, December 20 th 2018.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Operator Terminal Adapter (OTA):

OTA Hardware versions: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B;

OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5

to the Sponsor, Thales Norway AS, 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 ST [8] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

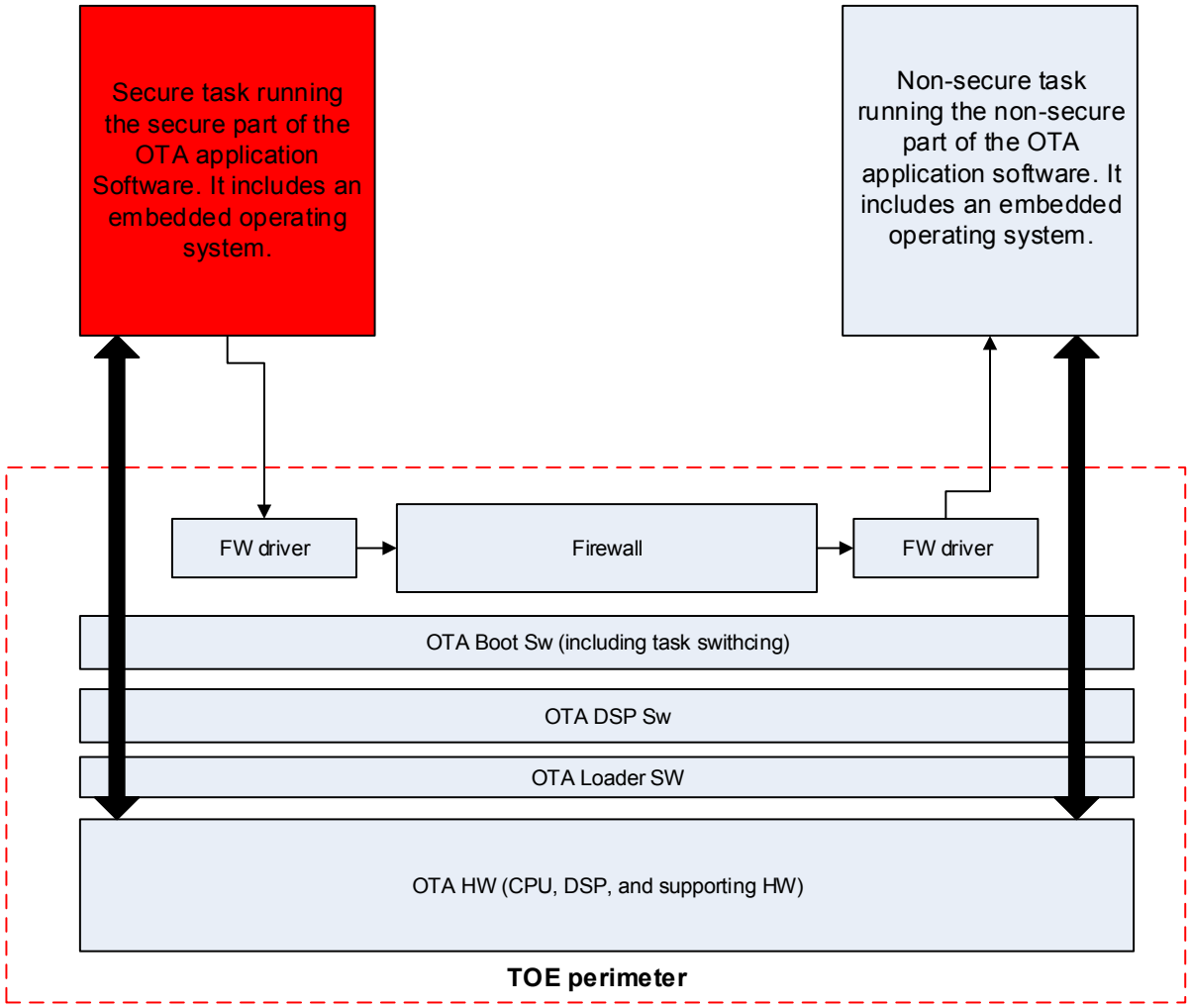
The product evaluated was Operator Terminal Adapter (OTA) with:

OTA Hardware versions: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B;

OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5.

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

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



4.3 TOE scope

The scope of the TOE is limited to the security functions in the Operator Terminal Adapter (OTA), comprising hardware and software as identified in chapter 0.

4.3.1 Outside the scope of evaluation

The OTA Application Software; all voice input/output sources/devices; Multifunction Terminal (MFT); panel comprising indicator lamps, loudspeaker etc. are not part of the TOE.

The TEMPEST certification is outside the scope of this evaluation.

4.4 Protection Profile Conformance

The ST [8] did not claim conformance to any protection profile/cPP.

4.5 Assurance Level

The ST [8] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 5 augmented with 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 [2].

4.6 Security Policy

Audio coupling of secure communications onto active non-secure lines at operator consoles shall be avoided in accordance with paragraph 35 and 37 in AC/35-D/2001-REV2, NATO Security Committee – Directive on Physical Security [15].

The TOE security policies are detailed in ST [8].

4.7 Security Claims

The ST [8] fully specifies the TOE's security objectives, the threats which these objectives counter 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. An overview of CC is given in CC Part 1 [2].

4.8 Threats Countered

The following threats are countered by the TOE:

- Classified information on a secure channel may be transferred to non-secure channel.
- Security-critical part of the TOE may be subject to physical attack that may compromise security.
- An attacker may send classified information from the secure to the non-secure network, by the use of call handling or management messages.
- System malfunctions may give the OCP user a wrong indication of whether the microphone is connected to a secure channel or a non-secure channel. The OCP user may then speak classified information on the non-secure network.
- The OCP user speaks classified information when the microphone is connected to the non-secure network.
- Microphones connected to non-secure channels may pick up classified speech.
- Electromagnetic emanations may divulge classified information.

- Authorised persons may perform unauthorized use of the operator position applications and management system inside the operation site.

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

- The OTA application will transmit alarms (if possible) to the management system (i.e. SMA).
- The periodic functions for abstract machine testing of the TOE are initiated from the OTA application.
- The VCS including the TOE must be installed accordingly to the installation guidelines. Only authorised persons shall be given physical access to the VCS. The TOE must be installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
- All users of VCS are fully trained to use, handle and interpret the VCS equipment. The technicians should be trained to install the VCS including the TOE accordingly to the installation guidelines.
- Only authorised persons shall be given physical access to the VCS. All OCP users have the minimum clearance for the maximum-security level of information handled in the system.
- Special authorisation is required to grant access to handle configuration and management of the VCS.
- The VCS including the TOE must be installed accordingly to the installation guidelines.
- All audit data is stored on a secure way and authorised users ensures that the logs are maintained and inspected on a regular basis, and ensures that proper action is taken on any breaches of security. The audit functionality is put outside the TOE.

4.11 TOE IT Security Objectives

- If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm indication and raise an alarm to the OTA application (required non-TOE SW) in order to send an alarm message to the management system. When the TOE operates in the mode “OTA in OCP”, the TOE shall also upon detection of failures on the security indicators (lamp panel), raise a local alarm indication and raise an alarm to the OTA application (required non-TOE SW) in order to send an alarm message to the management system.

- The TOE shall raise an alarm to the OTA application (required non-TOE SW) in order to send an alarm message to the management system when the threshold for traffic through the firewall is exceeded or when messages are rejected by the firewall.
- To prevent unacceptable acoustic cross-talk, the TOE shall ensure the following:
  - Secure channels shall be disconnected from the audio outputs when the voice transmission is activated and the microphone is connected to a non-secure channel to prevent unacceptable acoustic cross-talk of voice from secure channels to non-secure voice channels via audio devices connected to the TOE.
  - The microphone(s) shall be disconnected from non-secure channels when voice transmission is not activated.
  - The loudspeaker shall not be connected to secure channels.
- Remark to the term “unacceptable acoustic cross-talk”: The headsets and the use of the headsets shall prevent unacceptable acoustic cross-talk between earpiece and microphone of the headsets. The TOE shall cover all other potential cases of acoustic cross-talk of voice from secure channels to non-secure voice channels via audio devices connected to the TOE.
- Classified information shall be prevented from being transmitted on non-secure channels.
- The TOE shall ensure that only secure (valid) values are accepted for security attributes that are received from the environment.
- Information transmitted on secure voice channels shall not be transferred to non-secure voice channels.
- Security critical functions shall be tested by a combination of power-up tests, periodic tests and/or continuous tests.
- The OCP user shall unambiguously be made aware whether the microphone is connected to a non-secure channel.

4.12 TOE Non-IT Security Objectives

- The TOE shall be sealed in such a way that it is easy to see that it has been opened/tampered with.
- TEMPEST evaluation and certification of the TOE is performed by NSM. This certification ensures that NO.TEMPEST is achieved. This aspect is not treated further in this document.

4.13 Environment IT Security Objectives

- The management system shall receive auditable events from the TOE and provide facilities to securely store the audit data and present them for authorised management operators.
- Special authorisation is required to grant access to handle configuration and management of the VCS.
- The management system shall receive alarms from the TOE and present them for the management operator.
- The voice from the OCP shall be recorded.
- The periodic test of the firewall in the TOE shall be initiated from the OTA application.

4.14 Environment Non-IT Security Objectives

- Only authorised persons shall be given physical access to the VCS.
- Authorised users of the audit facilities must ensure that the audit facilities are used and managed effectively. On particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.
- The TOE shall be treated as a CCI material.
- All OCP users shall have a minimum clearance for the maximum-security level of information handled in the system.
- The responsible for the TOE must ensure that the VCS including the TOE are installed accordingly to the installation guidelines for the VCS.
- The VCS managers are fully trained to use and interpret the management application for the TOE.
- Each OCP user shall be made aware of ongoing non-secure transmission on the neighbouring OCPs. Operational procedures, not technical solutions, shall regulate concurrent use of classified and unclassified conversations to prevent acoustic cross-talk of classified conversations to be transmitted on unclassified communication channels.
- The VCS site shall have physical protection, which is minimum approved for the highest level of information handled in the system.
- The OCP users are fully trained to use the OTA and interpret the lamps on the LOL.

4.15 Security Function Policy

The TOE provides the following functional security components

- Security alarms (FAU_ARP.1(1))
- Security alarms (FAU_ARP.1(2))
- Complete information flow control (FDP_IFC.2)
- Simple security attributes (FDP_IFF.1)
- Illicit information flow monitoring (FDP_IFF.6)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Failure with preservation of secure state (FPT_FLS.1)
- Passive detection of physical attack (FPT_PHP.1)
- TSF self test (FPT_TST.1)
- Trusted path (FTP_TRP.1)

4.16 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 [1]. 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 both the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, CCRA [7], and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOGIS MRA [6] and the evaluation was conducted in accordance with the terms of these Arrangements.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST [8], which prospective consumers are advised to read. To ensure that the ST [8] 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 EAL5 assurance package as defined in Common Evaluation Methodology (CEM) [5].

For the evaluation of Operator Terminal Adapter (OTA), the Evaluators addressed every CEM [5] EAL 5 work unit augmented with ALC_FLR.3.

SERTIT monitored the evaluation in accordance with SD001E [1] which was carried out by the System Sikkerhet AS Commercial Evaluation Facility

(EVIT). The evaluation was completed when the EVIT submitted the final ETR [9] to SERTIT in 24.06.2019. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the ST [8] with reference to the assumed operating environment specified by the ST [8]. 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 augmented with ALC_FLR.3.

Assurance class	Assurance components	
ADV: 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	Semi-formal modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: 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
ASE: 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
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

AVA: Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the ST [8]. The results of this work were reported in the ETR [9] 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.

All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the certified version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The TOE is treated as CCI equipment, and is distributed according the Norwegian crypto security regulation, Forskrift om kryptosikkerhet [16].

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the guidance documents provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

The evaluators have examined and concluded the guidance documentation adequacy describes how the user can handle the TOE in a secure manner.

The evaluator examined the evidence and determined that the user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or that it is misleading or unreasonable.

A list of the guidance documents are given in chapter 3 References and Annex A.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always

follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 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 evaluator examined the evidence and determined that the test configurations were consistent with the configurations under evaluation as specified in the Security Target [8], and that the installation and configuration of the TOE (according to the documentation) at Thales Norway AS site in Oslo 20.02.2019 were done properly and were in a known state, and the set of resources were equivalent to the resources used by the developer to functionally test the TSFs. As a result, the evaluator determined that all requirements for this activity were satisfied.

The evaluator has devised eight penetration tests based on the evaluator's vulnerability analysis. The evaluator produced penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. All scenarios from the penetration testing were successfully performed with the expected results.

Further, the results of the penetration testing demonstrated that the TOE is resistant to an attacker possessing a moderate attack potential.

5.6 Developer's Tests

The developer has thoroughly tested the TSFIs and the TSF modules of the TOE.

This testing were divided in three parts:

- TSFI testing was performed for the functions firewall and red/black separation. Because the TSFIs are external interfaces to the modules, the tests were logical divided in two main parts like: test of the external interfaces to respectively the Firewall module and the Select Audio module. 25 different tests were performed.
- Software testing was performed on the Firewall module. The main functions of the Firewall module were tested, i.e. messages compliance, threshold validation, and alarm settings. 3 different tests were performed.
- Hardware testing was performed on the Select Audio module (and other HW features). The main functions of the Select Audio module were tested, i.e. voice processing and red/black separation performing. (The

other test features/areas were connectors, marking/identification, power supply, LEDs, reliability/maintainability, packing documentation, and manufacturing). 23 different tests were performed.

5.7 Evaluators' Tests

5.7.1 Sample testing

The evaluation team decided to perform the testing on both modules for sample testing:

- Firewall module
- Select Audio module

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

- NSecFromAudio
- SecFromAudio
- LampControl
- VoiceSelectAck
- SecDataToFW
- DataFromFW

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

- Security Function testing, to cover the TSFIs for the functions firewall and red/black separation.
- Software testing, to cover the Firewall module
- Hardware testing, to cover the Select Audio module (primary)

The modules and interfaces were verified through actual testing at the Thales Norway AS in Oslo 20.02.2019.

The test subset constituted about 27% of the total developers' tests, which is considered as sufficient sample testing. The test subset is described in the ETR [9]. The test configuration is described in Annex A. All scenarios from the sample testing have been successfully performed with the expected results.

5.7.2 Devised testing

The evaluation team decided to perform the testing on both modules for devised testing:

- Firewall module

- Select Audio module

The evaluation team decided to perform the testing on the following modules for devised testing:

- LampControl
- SecDataToFW
- DataFromFW

The modules and interfaces were verified through actual testing at the Thales Norway AS in Oslo 20.02.2019. All scenarios from the devised testing have been successfully performed with the expected results, and thus the devised tests have been verified by the evaluation team.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Operator Terminal Adapter (OTA),

OTA Hardware versions: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B;

OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5

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.

6.2 Recommendations

Prospective consumers of Operator Terminal Adapter (OTA),

OTA Hardware versions: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B;

OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5

should understand the specific scope of the certification by reading this report in conjunction with the ST [8]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST [8].

Only the evaluated TOE configuration should be installed. 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 included in the evaluated configuration.

There are no specific remarks regarding the auditing and testing of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Operator Terminal Adapter (OTA):

- OTA Hardware versions: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B;
- OTA trusted kernel: 3AQ 24860 AAAA Version 6.2.5

Developer: Thales Norway AS.

TOE Documentation

The supporting guidance documents evaluated were:

[a] Security Target for OTA [8],

[b] Guidance to Security Officer [10]

[c] Technical Manual [13],

[d] VCF Operator Position Manual [14].

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

TOE Configuration

The OTA used during evaluation/testing is delivered from the production line (KITRON) with preinstalled and tested (integrity) software and tested hardware (Off-line test), but the physical sealing was removed during testing.

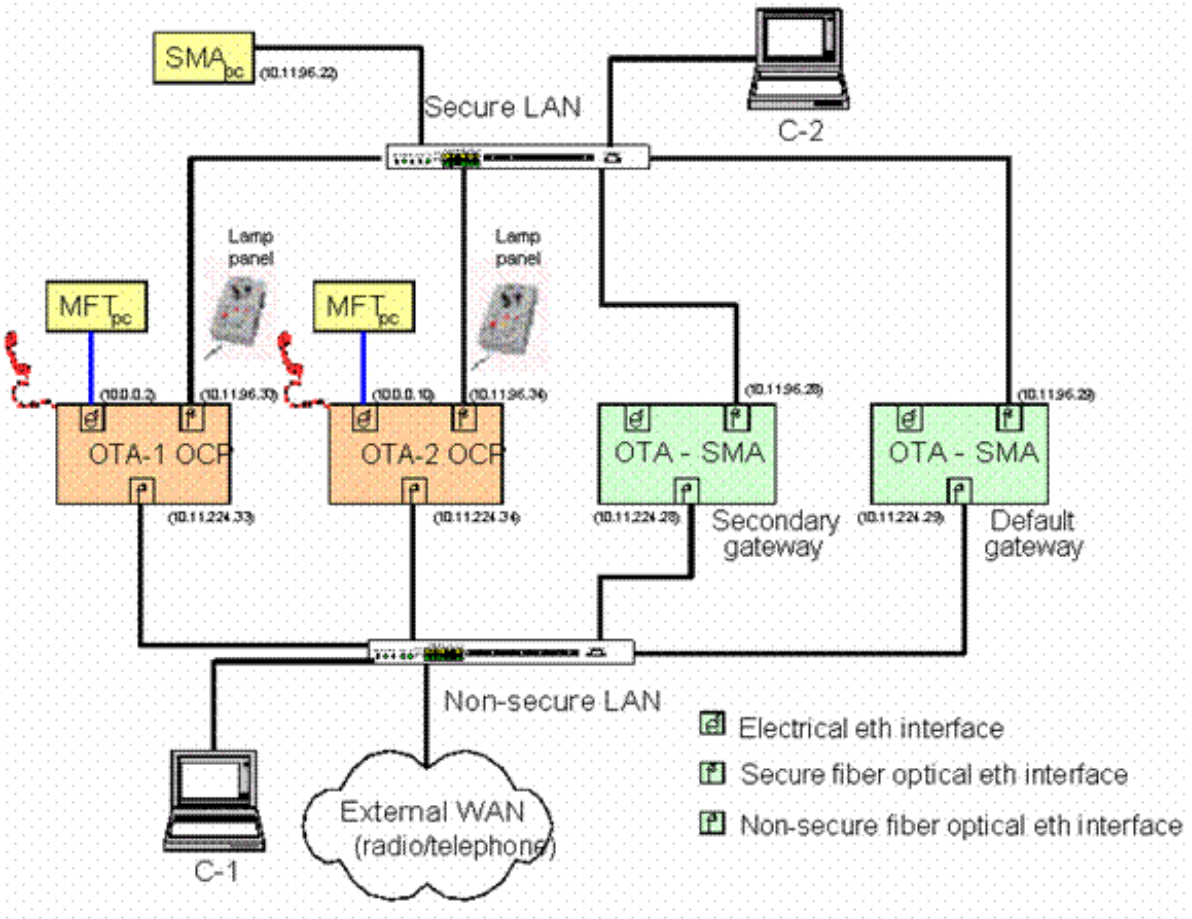
The evaluated/tested configuration consists of two OTA configured as OTA for SMA and two OTA in OCP. The configuration is performed through a Web browser (MS Internet Explorer) from a PC (SMA PC) in the Secure LAN. To each of the OTA in OCP mode there is connected an MFT PC, which performs/simulate the MFT functions, and a lamp panel.

The following configuration was used for testing:

SMA-PC	Type:	Dell OptiPlex GX 380
	Hardware:	Intel Core2 Duo: 3,0Ghz - 2,99GHz, 8G RAM
	OS:	Windows Server 2008 R2 Standard
	SW:	SMA 3AQ 13141TPAA 2.4.30, Thales
MFT 1 PC	Type:	IEI Technology, model: AFL-15A-N270/R/1G-R22

	Hardware:	Main board AFLMB2-945GSE(E248), Intel CPU N270, 1.6 GHz, 1016 MB RAM
	OS:	Linux CentOS 6.9
	SW:	TMF-A1-LOC-TMF-3.3.10, 2.4.6
MFT 2 PC	Type:	IEI Technology, model: AFL-15A/B-915-R11
	Hardware:	Main board AFLMB-9152-R11(E194), Intel Celeron M, 1.0 GHz, 1016 MB RAM
	OS:	Linux CentOS 6.9
	SW:	TMF-A1-LOC-TMF-3.3.10, 2.4.6
Lamp panel	Type:	Loudspeaker & Lamp 3AQ 21720 AAAA
Secure LAN switch	Type:	Nortel 4526T/4526FX/4524GT
Non-secure LAN switch	Type:	Nortel 4526T/4526FX/4524GT
C1 – developer	Type:	Lenovo T430
	Hardware:	Intel Core i5-3320M 2,6GHz 8 GB RAM
	OS:	Windows 7 Enterprise, Serv. Pack 1
	SW:	Wireshark v.2.2.1
	SW:	Tera Term v. 4.87
C1 was connected to Serial port to watch OTA-trace during the testing		
C1 was used for IND testing		
C2 – developer	Type:	Lenovo X201
	Hardware:	Intel Core i3 M390 2,67 GHz 2048 MB RAM
	OS:	Centos 7.7.1804
	SW:	fwmoduletest003.c
C2 was used for IND testing		

C1/C2 – evaluator	Type:	Lenovo T560
	Hardware:	Intel Core i7 16GB RAM
	OS:	Kali Linux 2019.1a
	SW:	hping3 version 3.0.0-alpha-2
	SW:	Nmap 7.70
	SW:	PortSwigger Burp Suite Pro 2.0.13beta
	SW:	Tenable Nessus Professional 8.2.3(#186) Linux Plugin set 201902181242
C1/C2 was used for VAN testing		



More information on the intended TOE environment can be found in the ST [8].