SERTIT

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

SERTIT-126 CR Certification Report

Issue 1.0 31 May 2024

Expiry date 31 May 2029

Thales Operator Terminal Adapter (OTA)
OTA Trusted Kernel: 3AQ 24860 AAAA version 6.2.7
OTA hardware: 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B

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

The Thales Operator Terminal Adapter (OTA) is part of the Voice Communication System (VCS) used in operation sites. The main purpose of the OTA is to provide the 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.

Thales OTA with

Trusted kernel version

- 3AQ 24860 AAAA version 6.2.7

Hardware versions

- 3AQ 21564 AAAA ICS7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ICS7B
- 3AQ 21564 AAAA ICS8
- 3AQ 21564 AAAA ICS8A
- 3AQ 21564 AAAA ICS8B

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 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 [9] with reference to the assumed operating environment specified by the ST [9]. 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.

This evaluation was a re-evaluation of the OTA because of a minor change/improvement of the TOE, and the scope was limited because only a minor set of documents were updated.

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 [9] which specifies the functional, environmental and assurance evaluation components.

The version of the product evaluated was Thales OTA with Trusted kernel version 3AQ 24860 AAAA version 6.2.7 and Hardware versions 3AQ 21564 AAAA ICS7, ICS7A, ICS7B, ICS8, ICS8A, ICS8B

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

The OTA is part of the Voice Communication System (VCS) used in operation sites. The Operator Controller Position (OCP) in the VCS are used by the operators to communicate with aircraft and naval forces afloat via G-A-G or G-M-G radio, other site operators, higher and lower echelons and other authorities and subscribers via G-G communications.

The VCS provides secure and non-secure voice communications to operators in the operation sites, between operators and external military and civilian networks and between operators and radios where that is required. The system is designed to provide a continuous 24 hours operation 7 days a week during times of peace, crisis/tension and war.

The main purpose of the OTA is to provide the capabilities required to handle all voice presented at the OCP and to perform the required red/black separation of voice and data. The OTA connects each OCP to both the secure and non-secure switching networks. The OTA is also used between the management system and the secure / non-secure switching networks so that the management system can manage both the secure and non-secure part of the VCS.

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, nine assumptions are made in the ST [9]. In order to counter eight threats as described in the ST [9], 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 5 augmented with ALC_FLR.3.

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

The evaluation activities were monitored by the certification team. 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 [9] and the ETR [10].

2 TOE overview

Figure 1 below shows the OTA in the VCS.

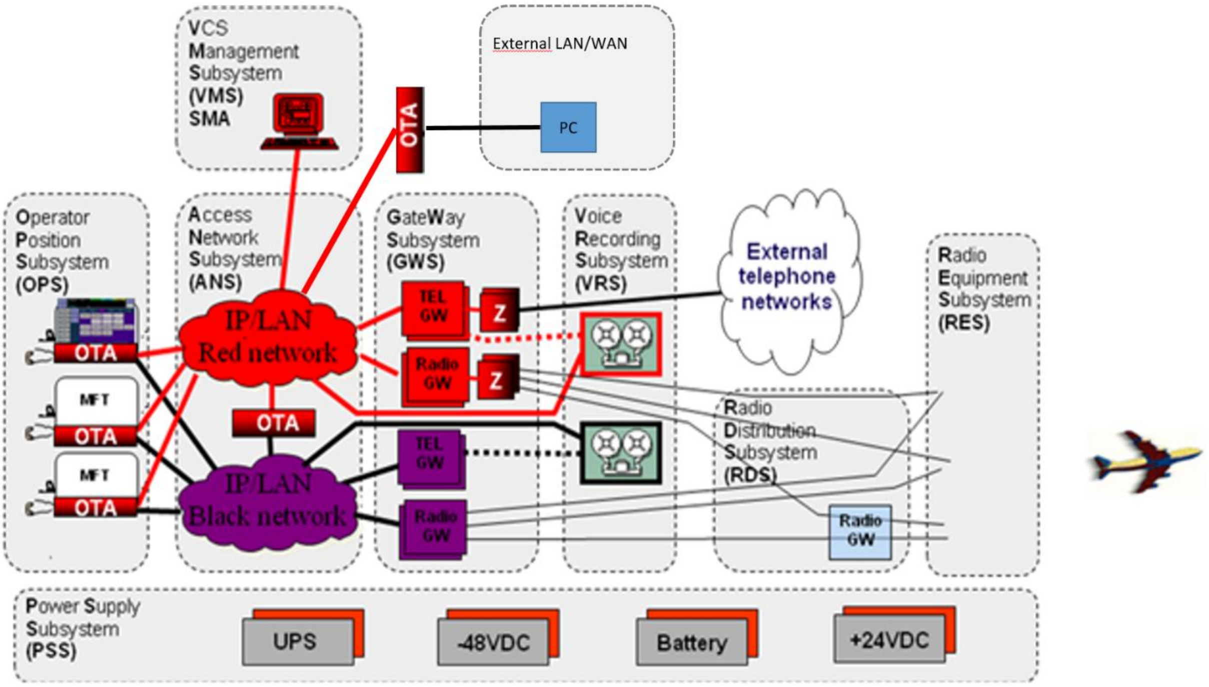
VCS Management Subsystem (VMS) SMA
OTA
External LAN/WAN
PC
Operator Position Subsystem (OPS)
Access Network Subsystem (ANS)
GateWay Subsystem (GWS)
Voice Recording Subsystem (VRS)
External telephone networks
Radio Equipment Subsystem (RES)
OTA
IP/LAN Red network
TEL GW
Z
Radio GW
Z
MFT
OTA
OTA
MFT
OTA
IP/LAN Black network
TEL GW
Radio GW
Radio Distribution Subsystem (RDS)
Radio GW
Power Supply Subsystem (PSS)
UPS
-48VDC
Battery
+24VDC

Figure 1

OTA is used in four configurations in the VCS, namely:

- OTA in OCP (in the Operator Position Subsystem in figure 1).
- OTA for SMA (in the Access Network Subsystem in figure 1).
- OTA for recording mode (VRR-OTA, in the Access Network Subsystem). This mode is identical to the SMA mode.
- OTA for remote equipment mode (RIE-OTA, in the External LAN/WAN). This mode is identical to SMA mode.

The OTA has identical hardware and software in all configurations. The mode of operation is determined by an installation parameter. OTA in OCP mode has audio handling and must have a lamp panel connected in order to handle audio. OTA for SMA does not have audio handling and has no lamp panel connected.

2.1 Definition of TOE perimeter

The TOE is the parts of the OTA implementing the core security functions, which must be highly trusted. The TOE comprises:

- The complete OTA HW, and
- One software configuration item comprising a defined set of OTA software modules.

The TOE software consists of:

- The firewall including drivers (the FW configuration file is outside the TOE),
- Boot software and software loader, and
- The red/black separation software including task switching, and
- Digital Signal Processor (DSP) SW.

The configuration of the firewall is set when the TOE SW is compiled and linked, thus making the configuration fixed and not possible to change during runtime. To change configuration a new TOE SW must be loaded. The customized configuration parameters are read from a firewall configuration file which is part of the OTA application software, i.e. outside the TOE.
The OTA application software is running in the secure and non-secure software tasks as illustrated in Figure 2 showing the OTA architecture. The OTA application software is considered less security critical and is outside the TOE.

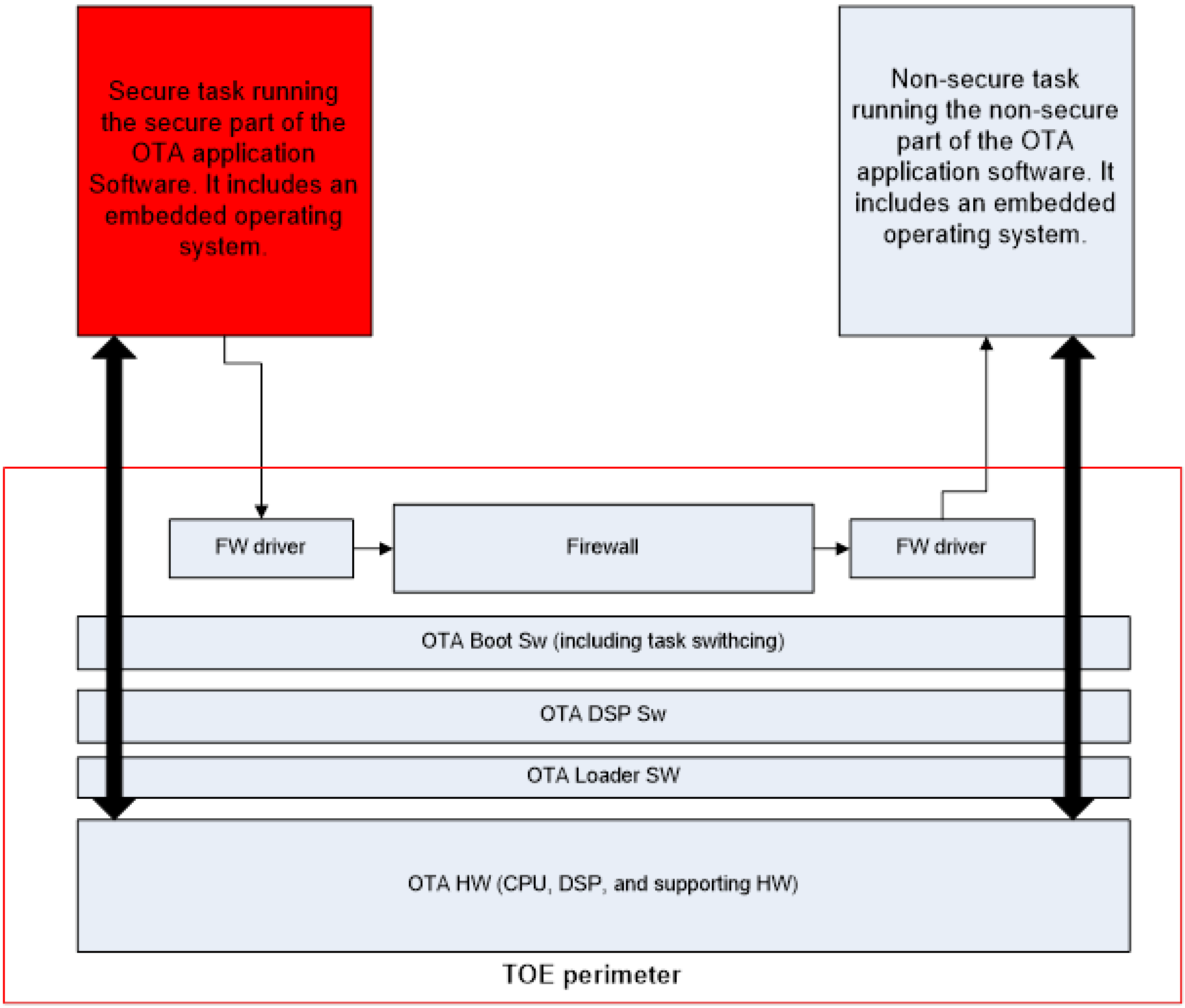
Secure task running the secure part of the OTA application Software. It includes an embedded operating system.
Non-secure task running the non-secure part of the OTA application software. It includes an embedded operating system.
FW driver
Firewall
FW driver
OTA Boot Sw (including task swithcing)
OTA DSP Sw
OTA Loader SW
OTA HW (CPU, DSP, and supporting HW)
TOE perimeter

Figure 2

2.2 TOE main characteristics and functionality

- The main functions of the TOE HW are to process voice, and to perform red/black separation.
- The TOE SW performs the following main functions:
  - Firewall
    - The firewall, which is configured at SW compile time by a customer specific firewall definition file, checks all messages from secure to non-secure domain (see figure 2) and accepts messages compliant with the preset configuration.
  - Red/black separation
    - Red/black separation is mainly achieved by separation of the secure (red) and non-secure (black) data and application SW in the OTA.
  - SW loader, HW initialisation, self-tests, start-up and task switching functions.
  - DSP with echo cancelling and VoX functions.

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
- VCS.COM
- USAGE
- AUDIT
- SELF.TEST
- OTA.ALARM

For details on these assumptions, the reader is advised to look at chapter 3.2 in the ST [9].

3.2 Threats Countered

The following eight threats are countered by the TOE:

- CINN.SEC.NON-SEC
- TAMPERING
- MISUSE
- WRONG.SEC.IND
- SEC.IND.MISSING
- ACOUSTIC.PICK-UP
- TEMPEST
- UNAUTHORISED.USE

For details on these threats, the reader is advised to look at chapter 3.3.4 in the ST [9]. The reader should also have a look at the description of the threat agents in chapter 3.3.3 in the ST [9].

3.3 Organisational Security Policies

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

- COUPLING

This policy is compliant with applicable parts of Norwegian security policy [14] and NATO security policy [15]. The TOE Organizational Security Policy is detailed in Chapter 3.4 of the ST [9].

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 analysis was conducted in the week of 26 February - 1 March 2024. 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 thoroughly tested the TSFIs and the TSF modules of the TOE.

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 4-8 March 2024.

5 Evaluated Configuration

The evaluated TOE, as described in Chapters 1, 2 and Annex A, is a combination of software and hardware.

Installation of the TOE must be performed completely in accordance with the guidance documents [11], [12], [13] provided by the developer. The TOE should be used in the operational environment as specified in the ST [9], as well as the guidance documents referenced in this chapter.

6 Evaluation Results

The evaluation addressed the requirements specified in the ST [9]. The ITSEF reported the results of this work in the ETR [10] on the 02 June 2023.

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	Semi-formal 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 [10], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the certification team, SERTIT has determined that Thales OTA 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 Thales OTA should understand the specific scope of the certification by reading this report in conjunction with the ST [9]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST [9].

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

The TOE should be used in accordance with the supporting guidance documentation [11], [12], [13] included in the evaluated configuration.

It should be noticed that unprotected exposure of the TOE might lead to the compromise of information or transmitted information (that could be classified or sensitive).

8 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
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
ITSEF	IT Security Evaluation Facility under the Norwegian Certification Scheme
OCP	Operator Controller Position
OTA	Operator Terminal Adapter
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SMA	Site Management Application
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 System
VoX	Voice Activation

9 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] Security Target, Security Target for OTA, 3AQ 24863 AAAA 377 EN ed. 6.2.10, 06 March 2024.

[10] (U) Evaluation Technical Report for OTA v1.1, 08 May 2024.

[11] Guidance to Security Officer Revision D, 13 June 2016

[12] (U) VCF Operator Position Manual, EdG

[13] Voice Communication System (VCS) Operator Terminal Adapter (OTA) Technical Manual, Ed9

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

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

Annex A: Evaluated Configuration

TOE Identification

Thales OTA with

Trusted kernel version

- 3AQ 24860 AAAA version 6.2.7

Hardware versions

- 3AQ 21564 AAAA ICS7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ICS7B
- 3AQ 21564 AAAA ICS8
- 3AQ 21564 AAAA ICS8A
- 3AQ 21564 AAAA ICS8B

Refer to the manufacturer’s documentation for additional information.

TOE Documentation

The supporting guidance documents evaluated were:

[a] Guidance to Security Officer, Revision D

[b] (U) VCF Operator Position Manual, EdG

[c] Voice Communication System (VCS) Operator Terminal Adapter (OTA) Technical Manual, Ed9

TOE Configuration

The following configuration was used for testing:

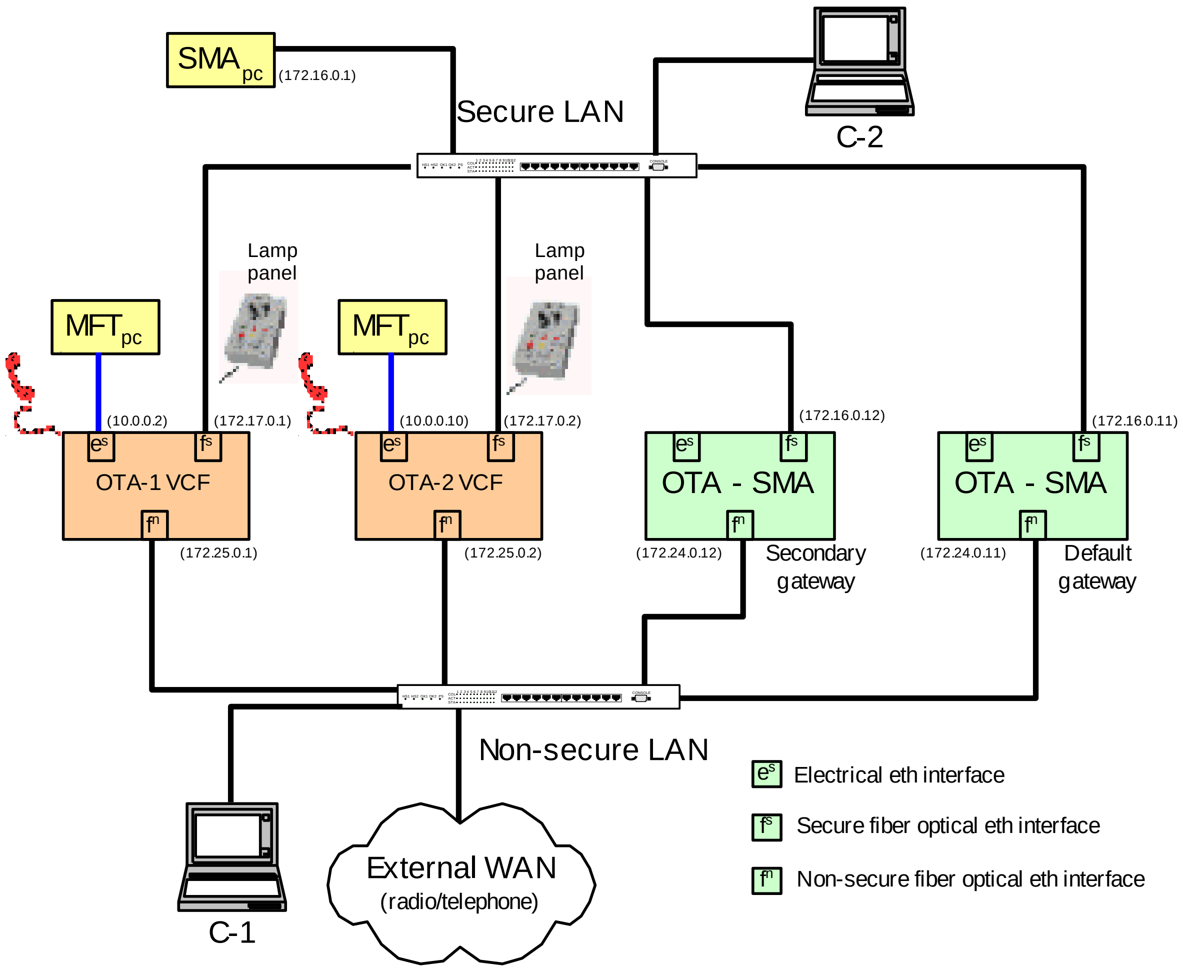

Figure 3