SERTIT-003 Certification Report

Issue 1.0 19. May 2004

Thales Operator Terminal Adapter (OTA)

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

Contents

1	**Certification Statement**	**3**
2	**Abbreviations**	**3**
3	**References**	**3**
4	**Executive Summary**	**3**
4.1	Introduction	3
4.2	Evaluated Product	3
4.3	TOE scope	3
4.4	Protection Profile Conformance	3
4.5	Assurance Level	3
4.6	Strength of Function	3
4.7	Security Policy	3
4.8	Security Claims	3
4.9	Threats Countered	3
4.10	Environmental Assumptions and Dependencies	3
4.11	TOE IT Security Objectives	3
4.12	TOE Non-IT Security Objectives	3
4.13	Environment IT Security Objectives	3
4.14	Environment non-IT Security Objectives	3
4.15	Security Functional Requirements	3
4.16	Security Function Policy	3
4.17	Evaluation Conduct	3
4.18	General Points	3
5	**Evaluation Findings**	**3**
5.1	Introduction	3
5.2	Delivery	3
5.3	Installation and Guidance Documentation	3
5.4	Misuse	3
5.5	Vulnerability Analysis	3
5.6	Developer's Tests	3
5.7	Evaluators' Tests	3
6	**Evaluation Outcome**	**3**
6.1	Certification Result	3
6.2	Recommendations	3
Annex A: Evaluated Configuration		**3**
TOE Identification		3
TOE Documentation		3
TOE Configuration		3
Environmental Configuration		3
Annex B: Product Security Architecture		**3**

Architectural Features 3

1 Certification Statement

Thales Operator Terminal Adapter (OTA) is a part of a Voice Communication System (VCS) used in operation sites. The main purpose of the OTA is to provide the capabilities required handling all voice presented at a Voice Communication Facility (VCF) and to perform the required red/black separation of voice and data.

The Operator Terminal Adapter with **software version 3AQ 21530 XAAA Version 2.9** and **hardware version 3AQ 21564 AAAA ICS5A** has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 requirements of Evaluation Assurance Level EAL 5 for the specified Common Criteria Part 2 functionality when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	19. May 2004

2 Abbreviations

CC	Common Criteria
CCI	Comsec Controlled Item
CCRA	Common Criteria Recognition Arrangement
CEM	Common Criteria Evaluation Methodology
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
MFT	Multi Function Terminal
NBC	Nuclear, Biological and Chemical
NDA Norway	National Distributing Authority Norway
NSM	Nasjonal sikkerhetsmyndighet (Norwegian National Security Authority)
OTA	Operator Terminal Adapter
POC	Point of Contact
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SMA	Site Management Application
SoF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VCF	Voice Communication Facility
VCS	Voice Communication System

3 References

[1] Operator Terminal Adapter Security Target, Edition 8, 05 March 2004, Reference 3AQ 21900 XAAA SCZZA Ed. 8. Thales Communications AS.

[2] Common Criteria Part 1, CCIMB-99-031, Version 2.1, August 1999.

[3] Common Criteria Part 2, CCIMB-99-032, Version 2.1, August 1999.

[4] Common Criteria Part 3, CCIMB-99-033, Version 2.1, August 1999.

[5] Om sertifiseringsordningen, Sd001, Versjon 3.0, 01.11.2002.

[6] Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, CEM-099/045, Version 1.0, August 1999.

[7] Common Criteria EAL 5 applied to multilevel interfaces in specific NDLO projects, Version 1/B, 03. April .2003.

[8] Recommendations for EAL 5, Version 1/-, 25. April 2002.

[9] Evaluation Technical Report, Issue 1.1, Document reference S-1506/20.06 29. April 2004.

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

[11] C-M(55)15(Final), Enclosure C, Security within the North Atlantic Treaty Organisation.

[12] Int. 003, Evaluation of Configuration Management (ACM_CAP.4), 11.02.2002.

[13] Int. 004, Evaluation of Configuration Management (ACM_SCP.3), 12.11.2001.

[14] Int. 008, Evaluation of ST, Introduction (ASE_INT.1), 31.07.2001.

[15] Int. 013, Evaluation of ST, IT security requirements (ASE_REQ.1) ,15.10.2000.

[16] Int. 016, Evaluation of Delivery (ADO_DEL.2), 11.02.2002.

[17] Int. 031, Evaluation of Vulnerability (AVA_VLA.3), 25.10.2002.

[18] Int. 049, Evaluation of ST, Security objectives (ASE_OBJ.1), 16.02.2001.

[19] Int. 064, Evaluation of ST, Explicitly stated IT security requirements (ASE_SRE.1), 16.02.2001.

[20] Int. 069, Evaluation of Development (ADV_SPM.3), 30.03.2001.

[21] Int. 074, Evaluation of coverage (ATE_COV.2), Evaluation of depth (ATE_DPT.2), 15.10.2000.

[22] Int. 075, Evaluation of functional tests (ATE_FUN.1), Evaluation of independent testing (ATE_IND.2), 15.10.2000.

[23] Int. 084, Evaluation of ST, IT security requirements (ASE_REQ.1), 16.02.2001.

[24] Int. 085, Evaluation of ST, IT security requirements (ASE_REQ.1), 11.02.2002.

[25] Int. 116, Evaluation of delivery (ADO_DEL.2), 31.07.2001.

[26] Int. 127, Evaluation of TOE summary Specification (ASE_TSS.1), 25.10.2002.

[27] Int. 128, Evaluation of Delivery (ADO_DEL.2), 15.11.2002.

[28] Int. 133, Evaluation of Vulnerability (AVA_MSU.2), 25.10.2002.

[29] Int. 138, Evaluation of ST, IT security requirements (ASE_REQ.1), 05.07.2002.

[30] Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) med endringer, sist ved lov av 21. desember 2001 nr. 117. ("Act relating to Protective Security Services")

[31] VCS OTA TECHNICAL MANUAL, 3AQ 12889 ABAA-EO, Ed. 1 – March-04

[32] VCS SMA OPERATOR MANUAL, 3AQ 12888 ABAA EO, Ed. 1 – March-04

[33] GUIDANCE TO SECURITY OFFICER AL1V-03-00682-B-P, Ed.B – 15 February-04

[34] SW REQUIREMENTS SPECIFICATION OTA-SRS-121, Ed. C – 28-May-03

[35] VCF OPERATOR POSITION OPERATOR MANUAL, N4244 06100100 354 1C Ed. C – 12. March-04

[36] OPERATOR TERMINAL ADAPTER (OTA) QUALIFICATION TEST SPECIFICATION, 3AQ 21564 AAAA QSZZA, Ed. 5 – 5-January-04

[37] OTA SECURITY DESIGN, PART 1 SYSTEM DESCRIPTION, 3AQ 21901 XAAA DEZZA, Ed. 7 – 4-February-2004

[38] OTA – OPERATOR TERMINAL ADAPTER INTEGRATION TEST SPECIFICATION, 3AQ 21530 XAAA QPZZA, Ed. 2.6 – 12-December-2003

[39] Shipment of CCI/Crypto material flow, Unnumbered.

[40] Mounting of NDA tampering label, 3AQ 21564 AAAA HDZZA, Ed. 2 – 2003.07.21

[41] Prosesser Levere Systemer, PRO 1015, Ed. 1 – 22-August-2003

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Operator Terminal Adapter with software version 3AQ 21530 XAAA Version 2.9 and hardware version 3AQ 21564 AAAA ICS5A,to the Sponsor, Thales Communications AS Norway, 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 [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was: Operator Terminal Adapter with software version 3AQ 21530 XAAA Version 2.9 and hardware version 3AQ 21564 AAAA ICS5A.

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

The TOE hardware provides connection for the audio devices, the loudspeaker, lamps and the Ethernet interfaces. The main functions of the TOE hardware are to process voice and to perform red/blacks separation.

The TOE software performs the following main functions: Voice handling, Routing, Firewall, Red/Black separation and Recording.

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

An overview of the TOE's security architecture can be found in Annex B.

4.3 TOE scope

The scope of the evaluation comprises the TOE software and hardware and that the TOE fulfils its security functions as described in the ST [1] section 6.1.

The following components of the Voice Communication Facilities (VCF) are outside of the scope of the evaluation:

- All voice input/output sources/devices.
- Multifunction Terminal (MFT).
- Panel with indicator lamps, loudspeaker, etc.

The tempest certification is not within the scope of the evaluation.

4.4 Protection Profile Conformance

The Security Target [1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 5 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7, where EAL 7 represents the highest assurance level. An overview of CC is given in CC Part 1 [2].

4.6 Strength of Function

The minimum Strength of Function (SoF) was SoF-High.

4.7 Security Policy

According to the ST [1], the TOE must be compliant with: Audio coupling of secure communications onto active non-secure lines at operator consoles shall be avoided in accordance with C-M (55)15 (Final) [11], Enclosure C, paragraphs 72 and 74. SERTIT would like to call attention to that this document is superseded by C-M(2002)49 [10] with supporting directives and guidance documentation.

4.8 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements (SFR) and security functions to elaborate the objectives.

All of the SFRs 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].

4.9 Threats Countered

The threats that the TOE counters are as follows:

- Classified information on a secure channel may be transferred to non-secure channels.
- 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 VCF user a wrong indication of whether the microphone is connected to a secure channel or a non-secure channel. The VCF user may then speak classified information on the non-secure network.
- The VCF 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 unauthorised use of the operator position applications and management system inside the operation site.

4.10 Environmental Assumptions and Dependencies

The following assumptions are assumed to exist in the environment:

- The VCS is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
- All VCF users are trained in the correct use of the VCS facilities.
- All VCF users have a minimum clearance for the highest security level of information handled in the system, and is authorised for all information handled by the system.
- Only users with special authorisation are allowed to do configuration and management of the system including TOE.
- The LANs in the VCS shall not be used for other communication than voice and signalling for call handling and system internal management communication.
- The TOE is used in the VCS and is installed according to the installation guidelines for the VCS.
- The audit functionality is handled outside the TOE.

4.11 TOE IT Security Objectives

The TOE IT security objectives in the ST [1] are as follows:

- If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm indication and if possible transmit an alarm to the management system (i.e. SMA). When the TOE operates in the mode "OTA in VCF", the TOE shall also upon detection of failures on the security indicators (lamp panel), raise a local alarm indication and transmit an alarm message to the management system.
- The TOE shall transmit an alarm message to the management system when the threshold for traffic through the firewall is exceeded or when a message is 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 VCF 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 non-IT security objectives in the ST [1] are met by procedural or administrative measures in the TOE's environment and are as follows:

- 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.

4.13 Environment IT Security Objectives

The environment IT security objectives in the ST [1] are as follows:

- 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.
- Voice from the VCF shall be recorded.

4.14 Environment non-IT Security Objectives

The environment non-IT security objectives in the ST [1] are as follows:

- 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 VCF 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 according to the installation guidelines for the VCS.
- The VCS managers are fully trained to use and interpret the management application for the TOE.
- Each VCF user shall be made aware of ongoing non-secure transmission on the neighbouring VCFs. 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 at least approved for the highest level of information handled in the system.
- The VCF users are fully trained to use the TOE.

4.15 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- 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
- Abstract machine testing FPT_AMT.1
- Failure with preservation of secure state FPT_FLS.1
- Passive detection of physical attack FPT_PHP.1

- TSF domain separation FPT_SEP.1
- Trusted path FTP_TRP.1

The IT-environment is required to satisfy the following SFRs:

- Security alarms FAU_ARP.1.Env
- Audit data generation FAU_GEN.1
- Potential violation analysis FAU_SAA.1
- Audit review FAU_SAR.1
- Protected audit trail storage FAU_STG.1
- Timing of authentication FIA_UAU.1
- Timing of identification FIA_UID.1
- Security roles FMT_SMR.1
- Reliable time stamps FPT_STM.1

4.16 Security Function Policy

The TOE has an information flow security function policy defined in FDP_IFC.2, FDP_IFF.1 and FDP_IFF.6. The information flow control provides flow control between the user interfaces and the secure and non-secure network and information flow control between the secure and non-secure network.

The flow control rules are based on:

- All messages from the secure network to the non-secure network are filtered in a firewall. If a message is rejected by the FW or the traffic through the FW exceeds the threshold value an alarm is generated.
- When there is a possibility that non-secure microphones may pick up from secure sources, the audio handling on the TOE will block secure audio to the audio devices.
- The TOE will prevent the microphones to be connected to the non-secure network in the case of a failing TOE security indicator.

4.17 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian IT Security Evaluation and Certification Scheme as described in SERTIT Document Sd001 [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT).

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] 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) [6] against the EAL 5 assurance package defined in CC Part 3 [4]. Interpretations used for EAL 5 are [7] and [8] listed in the reference section. Other interpretations used are [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28] and [29] listed in the reference section.

SERTIT monitored the evaluation which was carried out by the Secode System Sikkerhet ASA IT-Security Evaluation Facility (ITSEF/EVIT). The Task Start-up Meeting was held on 20. February 2003. 8 progress meetings were held and SERTIT also conducted an inspection of the evaluation facility, where the evaluation work was examined. The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR) [9] to SERTIT on 29. April 2004. SERTIT then produced this Certification Report.

4.18 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. 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

5.1 Introduction

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 5 assurance package.

Assurance class	Assurance components	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.3	Development tools CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.3	Semiformal functional specification
	ADV_HLD.3	Semiformal high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_INT.1	Modularity
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.2	Semiformal correspondence demonstration
	ADV_SPM.3	Formal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.2	Standardised life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_CCA.1	Covert channel analysis
	AVA_MSU.2	Validation of analysis

	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

The evaluation addressed the requirements specified in the Security Target [1]. 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

The TOE is treated as CCI equipment, and is distributed according to the Norwegian regulation "Forskrift om informasjonssikkerhet" § 7-1 to § 7-45 to the "Act relating to Protective Security Services" [30]. The distribution is described in § 7-19. NDA Norway has confirmed to the evaluators that the procedures for delivery of CCI material are used.

Related documents are Shipment of CCI/Crypto Material Flow [39], Mounting of NDA tampering label [40] and Prosesser Levere Systemer [41].

The TOE is sent by a courier or other methods approved by NSM if it is sent abroad. If the TOE is not sent by courier the sender shall notify the receiver on how the TOE is sent and when it can be expected to arrive.

If the TOE is sent within Norway the TOE shall be treated as NATO CONFIDENTIAL.

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.

5.3 Installation and Guidance Documentation

The developer performs all installation, generation and start-up. The evaluators has examined the guidance documents, [31], [32], [33], [34] and [35] and found that administrative functions, interfaces and how to administer the TOE in a secure manner are described.

Further more the evaluators have checked that the user guidance describes the functions and interfaces available to non-administrative users and the use of these functions are described.

A list of the guidance documents is given in annex A.

5.4 Misuse

Administrators should follow the guidance (see references in section 5.3 and in annex A) for the TOE in order to ensure that it operates in a secure manner. The guidance

documents adequately describe all possible modes of operation. Assumptions about the intended environment and external security measures are articulated. Sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions, and to detect insecure states.

5.5 Vulnerability Analysis

The evaluators were satisfied that the developer's vulnerability analysis describes all obvious vulnerabilities and that it gives a rationale for why they are / are not exploitable in the intended environment for the TOE.

The Evaluators' vulnerability analysis was based on the visibility of the TOE given by the evaluation process.

The evaluators produced and conducted five penetration tests on the basis of the developer's vulnerability analysis, and the evaluators produced and conducted three penetration tests based on their independent vulnerability analysis.

5.6 Developer's Tests

The developer's tests are divided in three parts:

- Hardware tests, where many of the tests are automatic tests in the production line of the TOE. Many of these tests include the security functions, which are included in the hardware. Ref. [36].
- Self-tests, which are part of the implementation and are performed on start-up and as supervision. Ref. [37].
- System tests, which are performed on the actual version of both hardware and software. Ref. [38]

The test configuration is described in chapter 5 of [38].

The developer has thoroughly tested all security functions of the TOE, and the TOE will also be tested at the VCS-site before the VCS-system is handed over to a customer.

5.7 Evaluators' Tests

The evaluators focused their testing on the error conditions in the following security functions: SF.Security.Alarm, SF.Information.Flow.Control, SF.Security.Management, SF.Self.Test, SF.Fail.Secure, SF.Domain.Separation and SF.Trusted.Path. The only security function not selected for testing was the SF.Passive.Protection which describes that the TOE has a physical sealing. The evaluators tested a sample of 35% of the developers tests. The test subset is described in the ETR [9]. The test configuration is described in annex A.

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 version SW: 3AQ 21530 XAAA Version 2.9, HW: 3AQ 21564 AAAA ICS5A meets the specified EAL5 Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 5 for the specified Common Criteria Part 2 conformant functionality, in the specified environment.

The minimum Strength of Function was SoF-High.

6.2 Recommendations

Prospective consumers of Operator Terminal Adapter version SW: 3AQ 21530 XAAA Version 2.9, HW: 3AQ 21564 AAAA ICS5A should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target [1].

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

Annex A: Evaluated Configuration

TOE Identification

The TOE is uniquely identified as:

Thales Operator Terminal Adapter (OTA)

- Software version 3AQ 21530 XAAA Version 2.9
- Hardware version 3AQ 21564 AAAA ICS5A

TOE Documentation

The supporting guidance documents evaluated were:

- OTA Security Target [1]
- OTA Technical Manual [31]
- OTA Operator Manual [32]
- Guidance to Security Officer [33]
- SW requirements specification [34]
- VCF Operator Manual [35]

TOE Configuration

The following configuration was used for testing:

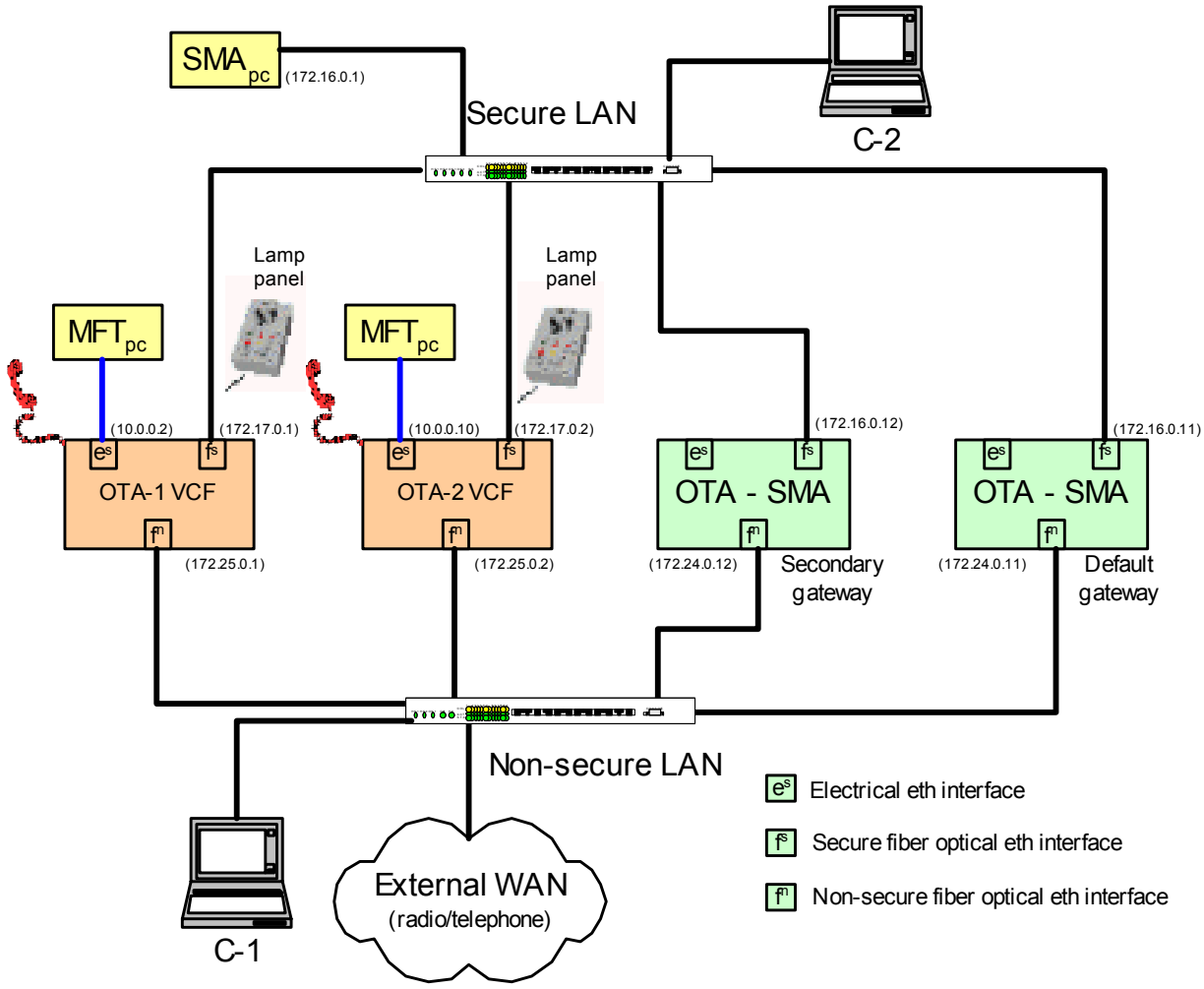

Figure 1 Evaluated configuration

The components used during evaluation/testing are:

SMA-PC:	Type:	Fujitsu Siemens, Celsius 400
	Hardware:	Intel Pentium 4, 2.4 GHz, 1G RAM
	OS:	Windows 2000, Service Pack 3
	SW:	Site Management Application, version 2.9, Thales
MFT 1 PC	Type:	Fujitsu Siemens, Scenic
	Hardware:	Intel Pentium 4, 2.4 GHz, 512 M RAM
	OS:	Red Hat Linux, release 7.3 Operating System Release 2.4.18-3
	SW:	MFT Software, version 2.6, Thales
MFT 2 PC:	Type:	TECH
	Hardware:	Intel Pentium 3, 550 MHz, 128M RAM

	OS:	Red Hat Linux, release 7.3 Operating System Release 2.4.18-3
	SW:	MFT Software, version 2.6, Thales
MFT 3 PC:	Type:	REC
	Hardware:	Intel Pentium 2, 128M RAM
	OS:	Windows NT
	SW:	MFT Simulator, Thales
MFT 4 PC	Type:	Fujitsu Siemens, Lifebook
	Hardware:	Celeron, 64M RAM
	OS:	Windows 98 Second Edition
	SW:	MFT Simulator, Thales
Lamp panel	Type:	Loudspeaker & Lamp3AQ 21720 AAAA
Secure LAN switch	Type:	HP LAN switch HPJ 4110A
Non-secure LAN switch	Type:	HP LAN switch HPJ 4110A
C1	Type:	hp compaq nx7000
	Hardware:	Intel Pentium M, 1,6 GHz, 1 GB RAM
	OS:	Linux Red Hat 9
	Software:	Nessus version 2.0.8, with signatures updated 27.01.2004
C2	Type:	hp compaq nx7000
	Hardware:	Intel Pentium M, 1,4 GHz, 256 MB RAM
	OS:	Windows XP Professional Version 2002 Service pack 1
	Software:	MS Office 2000

Environmental Configuration

The TOE HW provides connection for the audio devices, the loudspeaker and lamps and the Ethernet interfaces

The main functions of the TOE HW are to process voice, and to perform red/black separation. The TOE uses an external AC/DC converter. All connectors that may be used by VCF users are located at the front of the TOE; while all connectors intended to be handled by installation and maintenance are located at the rear end. The front end has also some indicator lamps providing information of the status of the TOE, the power and each of the Ethernet interfaces.

The VCF has both handset and headset, but only one at a time can be active.

The VCF supervisor feature is provided by use of a second headset. The voice from the microphone in one headset is sent back into the left ear of the other headset. The

microphone voice to be sent by the TOE towards the communication resources is a sum of the microphone voice from the two headset microphones.

The handset connector can also be used for a separate microphone. The intended use is for personnel wearing NBC gear. The headset connector #1 is then used to connect the headset.

The TOE is connected to secure and non-secure LAN by use of 100 Mb/s fibre optical Ethernet interface and can be connected to the MFT via a 10/100 Mb/s electrical Ethernet interface

The TOE software performs the following main functions:

- Voice handling
- Routing
- Firewall
- Red/black separation
- Recording

The VCS is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.

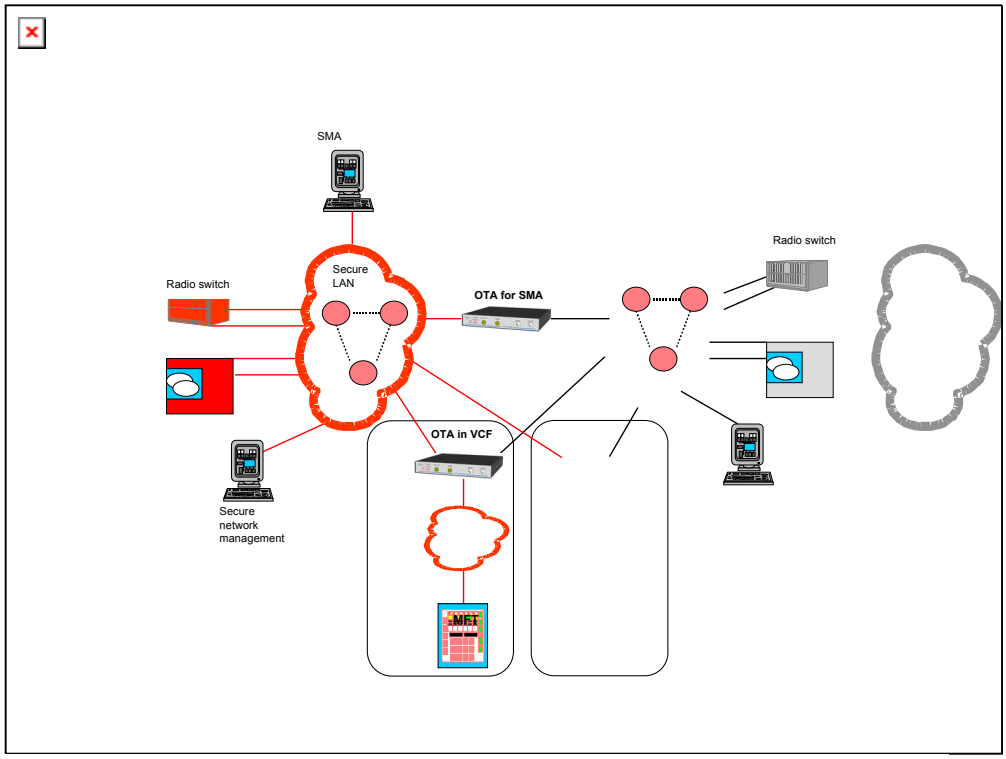

Figure 2 VCS Architecture

Annex B: Product Security Architecture

This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

The Voice Communication System (VCS) provides voice communication facilities to users of the Voice Communication Facilities (VCF) equipment located in operation sites. External communication networks and existing voice communication systems are used to provide connectivity for Ground-to-Ground (G-G), Ground-to-Air-to-Ground (G-A-G) and Ground-to-Maritime-to-Ground (G-M-G) voice communication being supported by the VCS. The VCS is designed to handle mixed secure and non-secure information, and to provide a continuous 24 hours operation 7 days a week during times of peace, crisis/tension and war.

A simplified illustration of the VCS and its external environment is given in **Figure 3**.

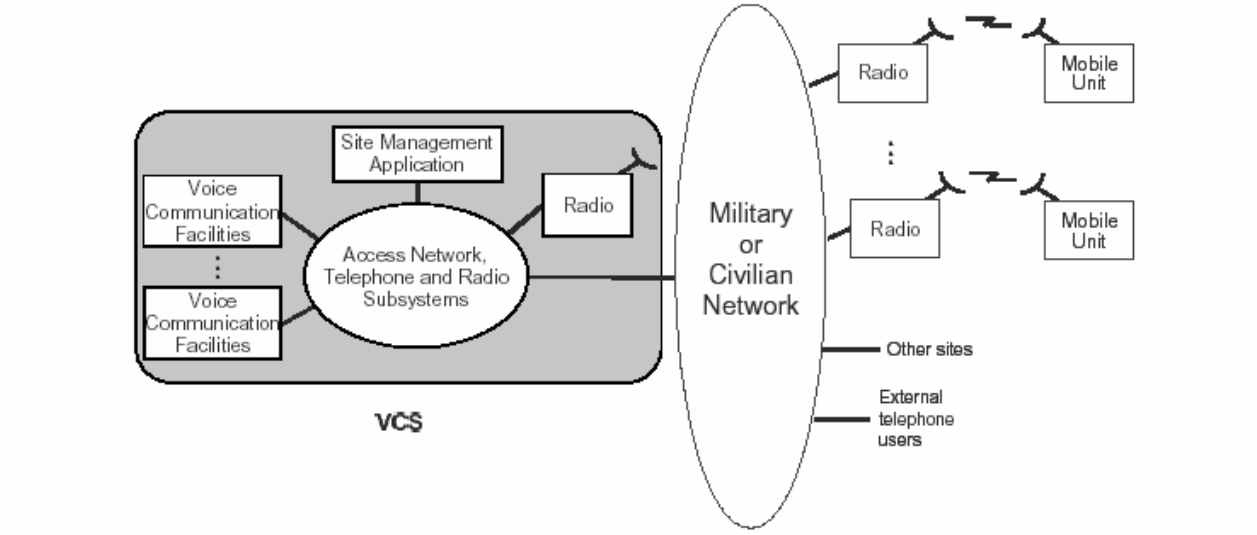

Figure 3: VCS simplified illustration

The VCS is a flexible system due to the switched access network and the modularity of the centralized switching systems. The centralized switching equipment, that is the access network, the telephone equipment and the radio control equipment, consists of small switching units connected together in a meshed network. This makes the system easy to reconfigure and easy to expand in order to obtain increased capacity.

The VCS provides the following voice communication services:

- Local and remote UHF/VHF/HF radios used by the VCF user for G-A-G and G-M-G voice communication. The radio communication can be non-secure (unencrypted) or secure (encrypted).

- The local G-G voice communication is offered to the VCF users in the form of telephone and intercom communication. Intercom communication makes use of direct access keys for user to user communication, while telephone communication makes use of both direct access keys and keypad. Local G-G voice communication is offered to standard telephone users as ordinary telephone communication. The local G-G voice communication can be non-secure or secure.
- The external G-G voice communication makes use of ordinary telephone communication via military, public and other private networks. The external G-G voice communication can be non-secure (unencrypted) or secure (encrypted).
- Loops are provided for the interconnection of VCF users with the same area of interest like Surveillance Loop, Weapons Loop etc. Local loops can be connected to external loops providing interconnection of VCF users with the same area of interest between VCS sites. Loops are normally non-secure.