



SERTIT-012 CR Certification Report

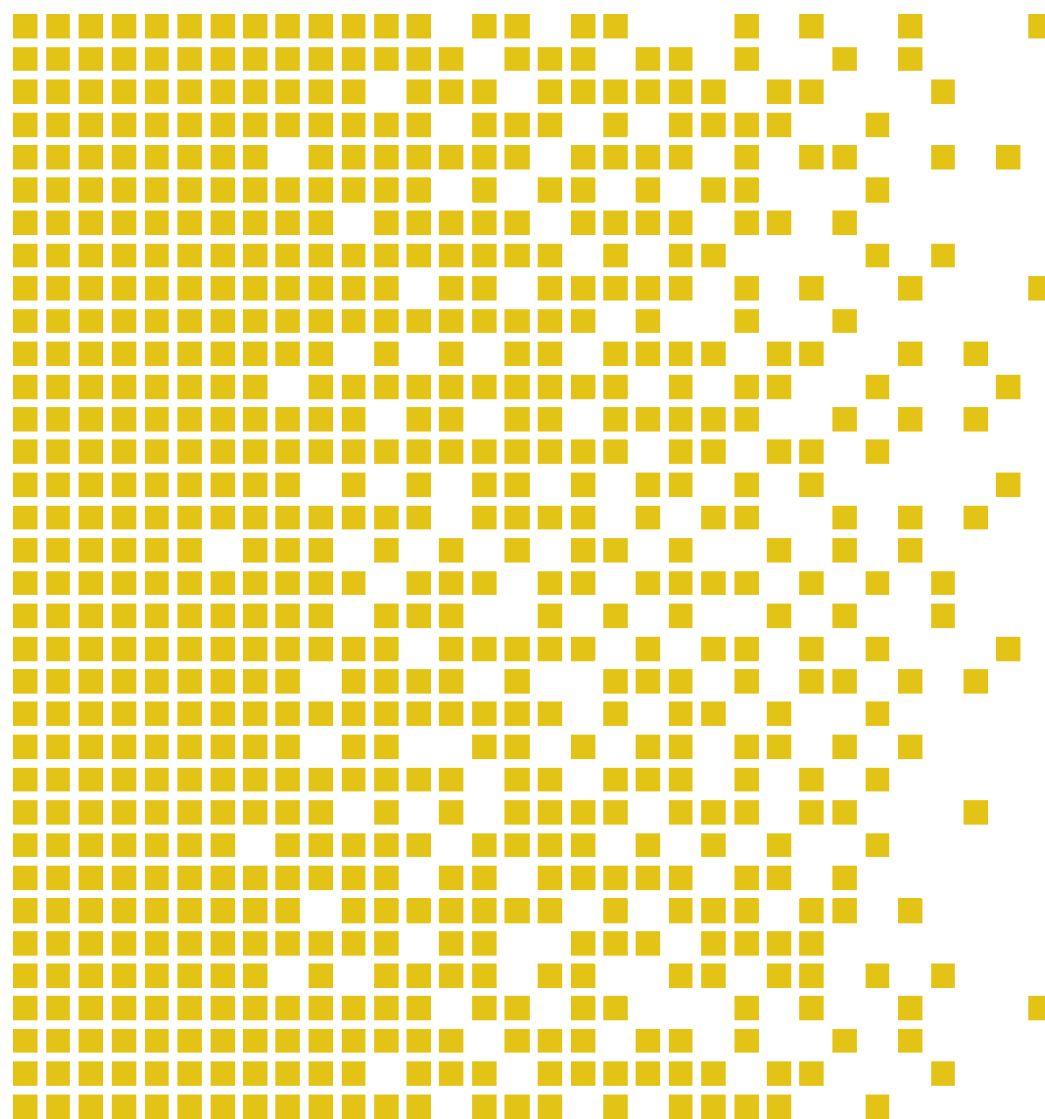
Issue 1.0 24 March 2010

Thales Operator Terminal Adapter

Trusted Kernel version 3AQ 24860 AAAA 6.2.1

Firewall definitions file 3AQ 24862 EAAA 6.2.2

Hardware version 3AQ 21564 AAAA ICS5A, -ICS7, -ICS7A and -ICS7B.



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.0 13.09.2007





Contents

	Certification Statement	4
1	Abbreviations	5
2	References	6
3	Executive Summary	7
	3.1 Introduction	7
	3.2 Evaluated Product	7
	3.3 TOE scope	7
	3.4 Protection Profile Conformance	8
	3.5 Assurance Level	8
	3.6 Strength of Function	8
	3.7 Security Policy	8
	3.8 Security Claims	8
	3.9 Threats Countered	8
	3.10 Threats and Attacks not Countered	9
	3.11 Environmental Assumptions and Dependencies	9
	3.12 TOE IT Security Objectives	9
	3.13 TOE Non-IT Security Objectives	10
	3.14 Environment IT Security Objectives	11
	3.15 Environment Non-IT Security Objectives	11
	3.16 Security Functional Requirements	12
	3.17 Security Function Policy	13
	3.18 Evaluation Conduct	13
	3.19 General Points	14
4	Evaluation Findings	15
	4.1 Delivery	16
	4.2 Installation and Guidance Documentation	16
	4.3 Misuse	16
	4.4 Vulnerability Analysis	17
	4.5 Developer's Tests	17
	4.6 Evaluators' Tests	17
	4.6.1 Devised testing	17
	4.6.2 Sample testing	18
5	Evaluation Outcome	19
	5.1 Certification Result	19
	5.2 Recommendations	19
	Annex A: Evaluated Configuration	20
	TOE Identification	20
	TOE Documentation	20
	Evaluation tools	20
	TOE Configuration	21

Certification Statement

Thales Operator Terminal Adapter (OTA) is a 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 required red/black separation of voice and data.

Thales OTA with

Trusted Kernel version

- 3AQ 24860 AAAA 6.2.1


Firewall definitions file

- 3AQ 24862 EAAA 6.2.2

Hardware versions

- 3AQ 21564 AAAA ICS5A
- 3AQ 21564 AAAA ICS7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ICS7B.

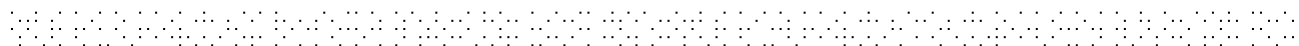
has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 conformant functionality when running on the platforms specified in Annex A.

Author	Arne Høye Røge Certifier 
Quality Assurance	Lars Borgos Quality Manager 
Approved	Kjell W. Bergan Scheme Director 
Date approved	24 March 2010



1 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
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
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
LOL	Loudspeaker and Lamps
MFT	Multifunction Terminal
OCP	Operator Controller Position
OTA	Operator Terminal Adapter
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
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
VCS	Voice Communication System



2 References

- [1] Operator Terminal Adapter Security Target, 3AQ 24863 AAAA SCZZA Ed. 6.2.2, 30 October 2009.
- [2] Common Criteria Part 1, CCMB-2005-08-001, Version 2.3, August 2005.
- [3] Common Criteria Part 2, CCMB-2005-08-002, Version 2.3, August 2005.
- [4] Common Criteria Part 3, CCMB-2005-08-003, Version 2.3, August 2005.
- [5] The Norwegian Certification Scheme, SD001E, Version 7.0, 28.3.2008.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2005-08-004, Version 2.3, August 2005.
- [7] Common Criteria version 2.3 – EAL5 Methodology, Version 4, 03.11.2006.
- [8] Evaluation Technical Report of the re-evaluation of the Operator Terminal Adapter – OTA, S22.86/20.06, 11.12.2009.
- [9] FOR 2001-07-01 nr 744: Forskrift om informasjonssikkerhet.
- [10] OTA Technical Manual 3AQ 24820 GAAA EO Ed.6.2.1 2009.11.02.
- [11] OTA Guidance to Security Officer 3AQ 24864 AAAA EOZZA Edition 6.1 27.08.2009.
- [12] ACEcom V6 Operator Control Position (OCP) User Manual 3AQ 41215 EAAA V6 Issue No. 001 2009.07.09.
- [13] Generic Failure Report 3AQ 24911 AAAA FB Edition 1.
- [14] OTA Security Design, Part 2 System Description, 3AQ 24863 AAAA DEZZA Part 2 Edition 6.2.1, 22.09.2009.
- [15] AVA_VLA-3.3E Evaluators vulnerability analysis Ver. 1.0.
- [16] SERTIT-003 CR Certification Report, issue 1.0, 19 May 2004
- [17] OTA Integration Test Specification and Log, 3AQ 21530 GAAA QPZZA, Ed. 6.2.2, 14.10.2009
- [18] OTA FW Module Test Results, 3AQ 21539 AAAA PK, Ed. 6.2.3, 05.11.2009
- [19] C-M(2002)49 Security Within the North Atlantic Treaty Organisation (NATO), 17. June 2002.

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Thales OTA 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 Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

3.2 Evaluated Product

The version of the product evaluated was Thales OTA with Trusted Kernel version 3AQ 24860 AAAA 6.2.1, Firewall definitions file 3AQ 24862 EAAA 6.2.2, Hardware versions 3AQ 21564 AAAA ICS5A, -ICS7, -ICS7A and -ICS7B.

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.

3.3 TOE scope

The scope of the TOE is limited to the Operator Terminal Adapter (OTA), comprising hardware and software as identified in chapter 3.2.

The following components of the Operator Controller Position (OCP) are outside of the scope of the evaluation:

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

This evaluation is a re-evaluation of the certified OTA software 3AQ 21530 XAAA version 2.9 and hardware 3AQ 21564 AAAA ICS5A. Certification Report Identifier is SERTIT-003 CR, issue 1.0, 19. May 2004 [16].

The re-evaluation comprises the security related changes made in the OTA software since the certified OTA software version 2.9. The OTA software is now split into three parts; i.e. the OTA Trusted Kernel software, the Firewall definitions file and the OTA application software. The OTA application software does not include any security functions and is not a part of the TOE.

The re-evaluated OTA hardware is the same hardware that was certified in the OTA evaluation (Certificate Identifier: SERTIT-003 C) and the TSF 101 evaluation

(Certificate Identifier: SERTIT-006 C) including some modifications. The modifications have been analysed in the appendix A to the ETR, "Security Justification of OTA changes MODIFICATION DESCRIPTION".

The TEMPEST certification is not within the scope of evaluation.

3.4 Protection Profile Conformance

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

3.5 Assurance Level

The OTA Security Target [1] specified the assurance requirements 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].

3.6 Strength of Function

The overall Strength of Function (SOF) claim was SOF-High. There are no SOF claims for specific TOE security functions.

3.7 Security Policy

The TOE must comply with Audio coupling of secure communications onto active non-secure lines at operator consoles shall be avoided in accordance with NATO document C-M(55)15(Final), Enclosure C, paragraphs 72 and 74. SERTIT would like to call attention to that this document is superseded by C-M(2002)49 [19] with supporting directives and guidance documentation.

3.8 Security Claims

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

All of 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].

3.9 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 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 unauthorised use of the operator position applications and management system inside the operation site.

3.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

3.11 Environmental Assumptions and Dependencies

The following assumptions are made for the environment:

- 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.

3.12 TOE IT Security Objectives

The TOE IT security objectives in the TSF 101 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 raise an alarm to the OTA application (environment) 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 (environment) in order to send an alarm message to the management system.
- The TOE shall raise an alarm to the OTA application (environment) 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.

3.13 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.

3.14 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.
- The voice from the OCP shall be recorded.

The periodic test of the firewall in the TOE shall be initiated from the OTA application.

3.15 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 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, 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.

3.16 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
- Abstract machine testing THA_REQ.1.Env
- Reliable time stamps FPT_STM.1



3.17 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.

3.18 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).

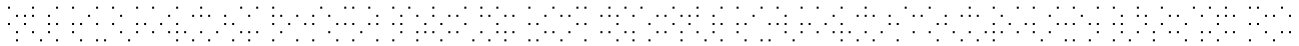
The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE 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].

Methodology used for EAL 5 is Common Criteria version 2.3 – EAL5 Methodology [7]

The Methodology for the EAL5 assurance level has been developed in relationship between Secode Norge AS, Norwegian National Security Authority (NSM) and Norwegian Defence Logistic Organisation/Sea (NDLO/SEA).

The TOE Security Functions (TSF) and security environment, together with much of the supporting evaluation deliverables, remained unchanged from that of Thales Operator Terminal Adapter software version 3AQ 21530 XAAA Version 2.9 and hardware version 3AQ 21564 AAAA ICS5A, which is previously certified by the Norwegian Certification Scheme for IT Security to the CC EAL 5 assurance level Certification Report Identifier is SERTIT-003 CR, issue 1.0, May 19th 2004 [16]. For the re-evaluation of Thales OTA, the evaluators addressed all work units but made some use of evaluation results where these were valid for both TOEs.

SERTIT monitored the evaluation which was carried out by the IT Security Evaluation Facility (ITSEF/EVIT), Secode Norge AS. 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) [8] to SERTIT 11.12.2010. SERTIT then produced this Certification Report.

3.19 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 organisation that recognises or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organisation that recognises or gives effect to this Certification Report is either expressed or implied.



4 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 ALC_FLR.3.

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_FLR.3	Systematic flaw remediation
	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 [8] 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.

4.1 Delivery

On receipt of the TOE, the consumer is recommended to check that evaluated versions of its constituent components have 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 regulation for information security, Forskrift om informasjonssikkerhet [9] § 7-1 to § 7-45. The distribution is described in § 7-19.

4.2 Installation and Guidance Documentation

The developer performs all installation, generation, and start-up. The evaluators have examined the guidance documents and determined that the administrative functions and interfaces and how to administer the TOE in a secure manner are described.

The evaluators also determined that the user guidance describes the functions and interfaces available to non-administrative users and the use of these functions.

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

4.3 Misuse

Administrators should follow the guidance for the TOE (see annex A) 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.

The firewall within the TOE software has configurable threshold values for each allowed protocol. The threshold values must be set a little higher than the traffic generated at normal operation, and higher than worst case traffic situations. However, the threshold should be set as low as possible so that potential misuse is detected. The [11] OTA Guidance to Security Officer describes the procedures for the calculation of the traffic thresholds.



4.4 Vulnerability Analysis

The evaluators found that each obvious vulnerability is described [14] and a rationale is given for why it is / is not exploitable in the intended environment for the TOE, and that the vulnerability analysis is consistent with the ST and the guidance documents for the TOE. The evaluator also determined that the developer search for TOE vulnerabilities is systematic.

The Evaluators' vulnerability analysis [15] was based on the visibility of the TOE given by the evaluation process.

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

4.5 Developer's Tests

The developer has thoroughly tested all security functions of the OTA.

In addition to the factory testing, which includes hardware testing and integrity testing of software, the OTA will be thoroughly tested at an OCP-site before the OCP-system is handed over to a customer.

The developer's tests are divided in three parts:

- Hardware tests, where many of the tests are performed as factory testing. The factory testing is automatic testing performed in the production line of the OTA. Many of these tests include the security functions, which are implemented in hardware. 67 tests are performed.
- Self-tests, which are part of the implementation, are performed at start up and as supervision. These tests are safeguarding the integrity of the security policy model of OTA. 122 tests are performed.
- System tests, which are performed on the actual version of both hardware and software. 67 tests are performed.

67 different tests are specified for the coverage of the security functions in OTA. These tests are part of both the hardware tests and the system tests.

4.6 Evaluators' Tests

4.6.1 Devised testing

The evaluation team decided to focus the testing on the error conditions in the security functions SF.Security.Alarm, SF.Information.Flow.Control, SF.Security.Management, SF.Self.Test and SF.Fail.Secure.

The security functions are verified through actual testing at Thales Norway AS.

The security functions that were not selected for devised testing are SF.Domain.Separation and SF.Trusted.Path, which are selected for testing during the sample testing and the SF.Passive.Protection, which describes that the TOE has a physical sealing.



4.6.2 Sample testing

The evaluation team decided to focus the selection of samples of the developers test on the error conditions in the security functions, SF.Security.Alarm, SF.Information.Flow.Control, SF.Self.Test, SF.Fail.Secure, SF.Domain.Separation and SF.Trusted.Path.

Most of these security functions are verified through testing at Thales Norway AS. The security functions SF.Domain.Separation and SF.Trusted.Path are verified through document inspection of software (source code) and hardware, as described in the developers testing approach.

The security functions that were not selected for testing are the SF.Security.Management, which is tested during the devised test subset and SF.Passive.Protection, which describes that the TOE has a physical sealing.

The developer have specified 67 different tests for testing of the security functions in OTA, the amount of samples selected for testing by the evaluation team is 24 different tests, which is 35,8% of the developers testing effort.

The test subset is described in the ETR [8]. The test configuration is described in annex A.



5 Evaluation Outcome

5.1 Certification Result

After due consideration of the ETR [8], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Thales OTA with Trusted Kernel version 3AQ 24860 AAAA 6.2.1, Firewall definitions file 3AQ 24862 EAAA 6.2.2, Hardware versions 3AQ 21564 AAAA ICS5A, -ICS7, -ICS7A and -ICS7B meets the Common Criteria Part 3 conformant requirements 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.

5.2 Recommendations

Prospective consumers of Thales OTA with Trusted Kernel version 3AQ 24860 AAAA 6.2.1, Firewall definitions file 3AQ 24862 EAAA 6.2.2, Hardware versions 3AQ 21564 AAAA ICS5A, -ICS7, -ICS7A and -ICS7B 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.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 3.3 "TOE Scope" and Section 5 "Evaluation Findings".

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



Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Thales OTA with

- Trusted Kernel version 3AQ 24860 AAAA 6.2.1
- Firewall definitions file 3AQ 24862 EAAA 6.2.2
- Hardware versions
 - 3AQ 21564 AAAA ICS5A
 - 3AQ 21564 AAAA ICS7
 - 3AQ 21564 AAAA ICS7A
 - 3AQ 21564 AAAA ICS7B

TOE Documentation

The supporting guidance documents evaluated were:

- OTA ST [1]
- OTA Technical Manual [10]
- OTA Guidance to Security Officer [11]
- ACEcom OCP User Manual [12]

Evaluation tools

During independent testing the developer's test bed was used, with components for the IT-environment, such as SMA and MFT programs on PCs with Windows and Linux operating systems.

For testing on the OTA firewall, a firewall test program developed by Thales Norway AS was used together with the corresponding test procedures OTA Integration Test Specification and Log [17] section 2.3 and OTA FW Module Test Results [18].

Test program name: FireWall TestProgram Edition 6.2.2

For penetration testing of the OTA the following tools were used from a PC running Mac OSx SnowLeopard version 10.6.1:

- Nessus version 3.2.1 (with plugins updated 06.10.2009)
- Nmap version 5.00
- Hping2 version 2.0.0-rc3
- Pentbox version 1.1-beta
- Wireshark version 1.2.2
- Colasoft Packet Builder version 1.0

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 a MFT PC, which performs/simulate the MFT functions, and a lamp panel.

The components used during testing are:

SMA-PC:	Type:	Dell Optiplex GX 280
	Hardware:	Intel Pentium 4, 2.8 GHz, 1G RAM
	OS:	Windows Server 2003, Service Pack 2
	SW:	SMA 3AQ 13141 EAAA 6.2.6, Thales
MFT 1 PC	Type:	IEI Technology Model: PAC 400GW/ACE-916AP
	Hardware:	Main board JUKI-6755, Intel Celeron, 1.2 GHz, 512 M RAM
	OS:	Linux CentOS release 2.6.18.53
	SW:	MFT 3AQ 13121 EAAA 6.2.2e, Thales
MFT 2 PC:	Type:	IEI Technology Model: PAC 400GW/ACE-916AP
	Hardware:	Main board JUKI-6755, Intel Celeron, 1.2 GHz, 512 M RAM
	OS:	Linux CentOS release 2.6.18.53
	SW:	MFT 3AQ 13121 EAAA 6.2.2e, Thales
Lamp panel Type:		Loudspeaker & Lamp 3AQ 21720 AAAA
Secure LAN switch Type:		HP ProCurve switch 2626 J4900A
Non-secure LAN switch Type:		HP ProCurve switch 2626 J4900A
C1	Type:	MacBook Pro
	Hardware:	Intel Core 2 Duo 2,8GHz, 4 GB DDR3 RAM,
	OS:	Mac OSx SnowLeopard v10.6.1
	Software:	Nessus 3.2.1, Plugins updated 06.10.2009 Nmap v5.00 Hping2 v2.0.0-rc3 Pentbox v1.1-beta Wireshark v1.2.2 Colasoft Packet Builder v1.0
C2	Type:	HP Compaq nc8430
	Hardware:	Intel Core 2 CPU T7200, 2,0 GHz, 2 GB RAM
	OS:	Windows XP Professional Version 2002 Service pack 3
	Software:	MS Office 2003 Wireshark Version 1.2.2 (SVN Rev 29910)

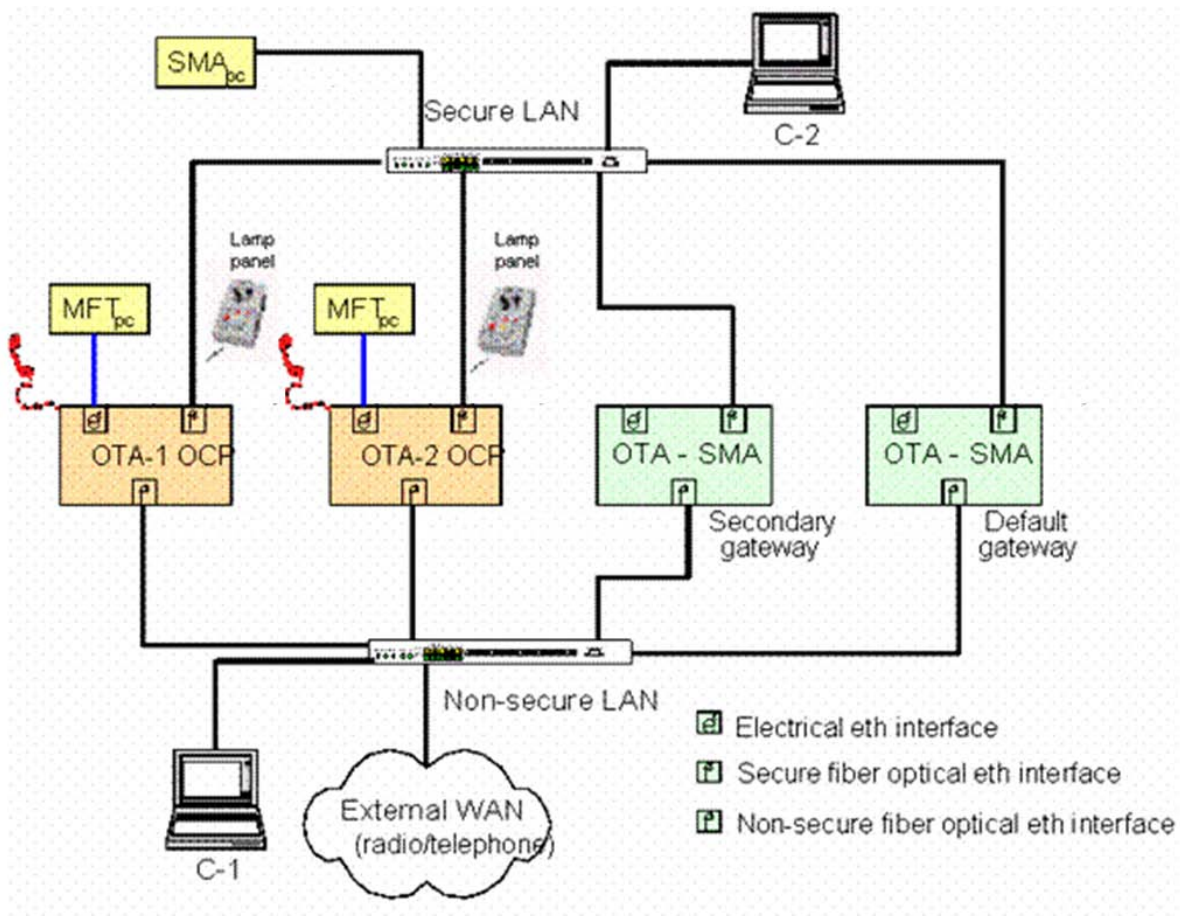


Figure 1 Test configuration

More information on the intended TOE environment can be found in the OTA Security Target [1]