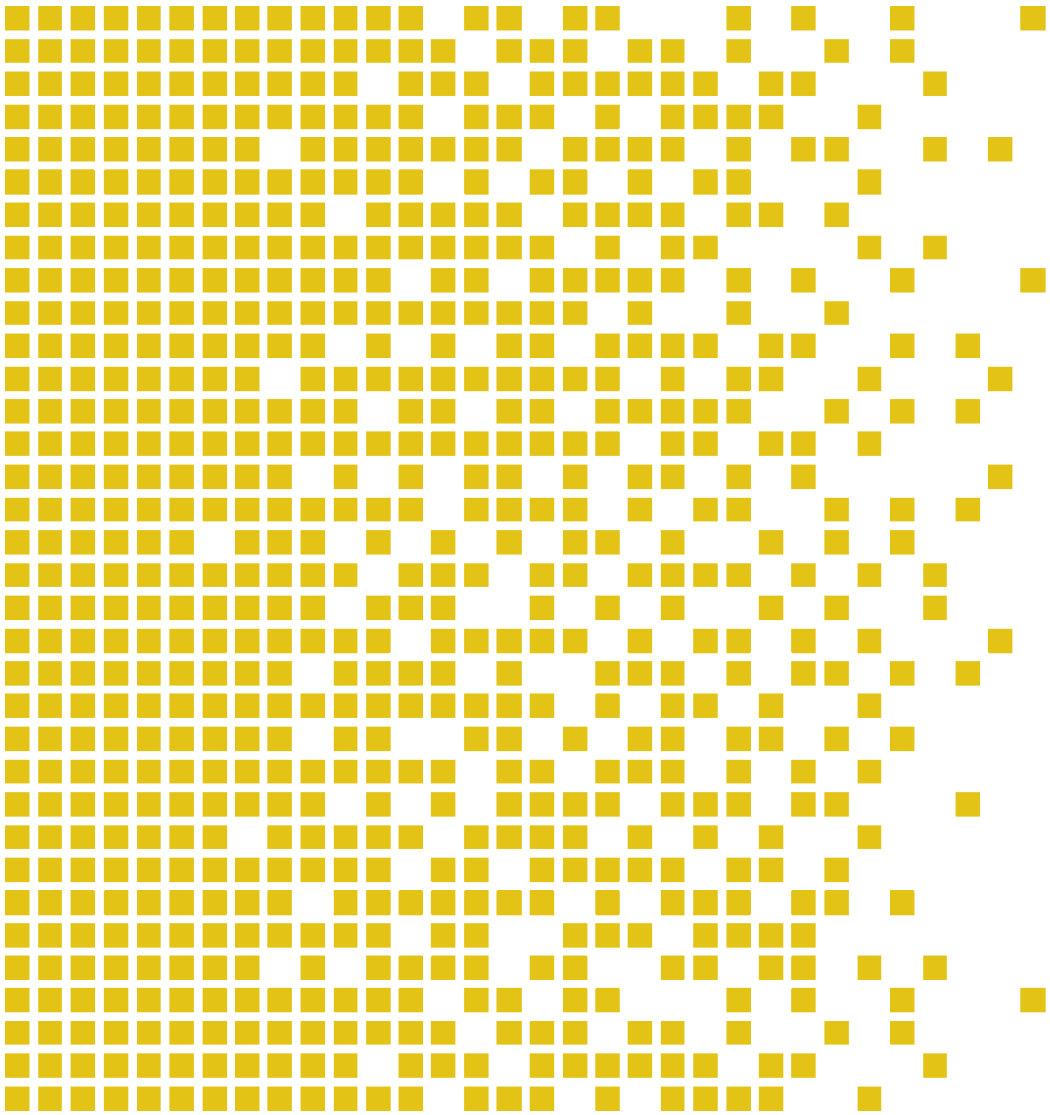
SERTIT-015 CR Certification Report

Issue 1.0 03 May 2010

Thales Trusted Security Filter - TSF101
Hardware versions: 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ISC7, -ICS7A and -ISC7B
Software version 3AQ 21850 CAAA Version 2.1.4



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

Thales Trusted Security Filter TSF101 is a filter whose main purpose is to filter a fixed and limited set of packet data between two networks of different security classification. Its design shall be trusted to perform red/black separation of data between a Secure and a Non-secure network in a highly specialized IT environment.

Thales Trusted Security Filter TSF101 with

Software version:

- 3AQ 21850 CAAA Version 2.1.4

Hardware versions:

- 3AQ 21564 AAAA ICS5
- 3AQ 21564 AAAA ICS5A
- 3AQ 21564 AAAA ICS6
- 3AQ 21564 AAAA ICS6A
- 3AQ 21564 AAAA ICS6B
- 3AQ 21564 AAAA ISC7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ISC7B

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 Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	03 May 2010

2 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	IT Security Evaluation Facility under the Norwegian Certification Scheme for IT Security
HCR	Helicopter radar system
ITSEF	IT Security Evaluation Facility
MSIFC	Multi Sensor Integration Fire Control
NAV	Navigation system
SERTIT	Norwegian Certification Authority for IT Security
SOF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSF101	Trusted Security Filter

3 References

[1] Trusted Security Filter Security Target, 3AQ 21840 AAAA SCZZA Ed. 2.2, 28 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, EvaluationMethodology, 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 Trusted Security Filter – TSF 101, S-2323/20.06, issue 1.2, 23 March 2010.

[9] SERTIT-006 CR, issue 1.0, 1 November 2007.

[10] FOR 2001-07-01 nr 744: Forskrift om informasjonssikkerhet.

[11] ACECom TSF Technical Manual 3AQ 21840 CAAA EQ, Ed. 1, 30.10.2009

[12] TSF 101 Software Installation Guide 3AQ 21850 XAAA BGZZA Ed. 2, 08.12.2006

[13] TSF 101 Security Design – Norwegian Frigates Part 2, 3AQ 21841 CAAA DEZZA Ed. 2.3, 27.01.2010

[14] AVA_VLA-3.3E Evaluators vulnerability analysis Ver. 1.0

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Trusted Security Filter TSF101 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.

4.2 Evaluated Product

The version of the product evaluated was Trusted Security Filter TSF101 with hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ISC7, -ICS7A and -ISC7B and software version 3AQ 21850 CAAA Version 2.1.4.

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 TSF101 comprising hardware and software as identified in chapter 4.2.

This evaluation is a re-evaluation of the certified TSF101 with software version 3AQ 21850 BAAA – 1.6, and hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ISC7, -ICS7A and -ISC7B. The Certification Report identifier is SERTIT-006 CR, issue 1.0, 1 November 2007 [9].

The TEMPEST certification is not within the scope of 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 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 Strength of Function

A Strength of Function (SOF) claim is not applicable for the TOE because there are no probabilistic or permutational TOE security functions.

4.7 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

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 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].

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 data messages.
- Electromagnetic emanations may divulge classified information.
- Authorised persons may perform unauthorised use of the system's applications and management system inside the operation site.

4.10 Threats and Attacks not Countered

It is not described any threats or attacks that are not countered.

4.11 Environmental Assumptions and Dependencies

The following assumptions are made for the environment:

- The system comprising the TOE and the connected networks is installed in a physical protected area, minimum approved for the highest security level of information handled in the system.
- All TOE managers are trained in the correct use of the TOE.

- All TOE managers 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 managers with special authorisation are allowed to do configuration and management of the system including TOE.
- The TOE is used between two LANs in a protected environment and is installed according to the installation guidelines for the TOE.

4.12 IT Security Objectives

The TOE IT security objectives are as follows:

- If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm.
- The TOE shall have an audit log that can be viewed by a web browser on the secure network.
- The TOE shall perform statistics registration of messages handled by the filter and provide facilities to present them for the TOE manager.
- Classified information shall be prevented from being transmitted on non-secure channels.
- Security critical functions shall be tested by a combination of power-up tests, periodic tests and/or continuous tests.
- The firewall filter shall not be configurable. The TOE manager shall be able to select sets of predefined filter criteria.
- The IT environment shall be able to display the web page with the firewall statistics. The web server resides in the TOE.
- Special authorisation is required to grant access to handle TOE firewall statistics.

The last two are Environmental IT Security Objectives.

4.13 Non-IT Security Objectives

The TOE non-IT security objectives 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.
- Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks.

- Authorised managers of the TOE must ensure that the TOE firewall statistics and audit log are used and managed effectively. On particular, TOE firewall statistics and audit log 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
- The TOE shall be treated as a CCI material.
- All 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 TOE is installed according to the installation guidelines for the TOE.
- The TOE managers are fully trained to use and interpret the TOE firewall statistics and audit log.
- The site where the TOE is installed shall have physical protection, which is minimum approved for the highest level of information handled in the system.

All objectives except the first two are Environmental Non-IT Security Objectives.

4.14 Security Functional Requirements

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

- Security alarms FAU_ARP.1
- Audit data generation FAU_GEN.1
- Security audit review FAU_SAR.1
- Protected audit trail storage FAU_STG.1
- Complete information flow control FDP_IFC.2
- Simple security attributes FDP_IFF.1
- Illicit information flow monitoring FDP_IFF.6
- Management of security attributes FMT_MSA.1
- Static attribute initialization FMT_MSA.3
- Specification of Management Functions FMT_SMF.1
- 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
- Reliable Time Stamp FPT_STM.1

The IT environment is required to satisfy the following SFRs:

- Potential violation analysis FAU_SAA.1
- Audit Review FAU_SAR.1.Env
- Timing of identification FIA_UID.1
- Security roles FMT_SMR.1

4.15 Security Function Policy

The TOE has an information flow security function policy defined in FDP_IFC.2, FDP_IFF.1, FMT_MSA.1 and FMT_MSA.3. 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.
- The TOE manager can select sets of predefined filter criteria.

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 [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 the evaluation of TSF101 with software version 3AQ 21850 BAAA – 1.6, and hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ISC7, -ICS7A and -ISC7B., which has previously been certified by the Norwegian Certification Scheme for IT Security to the CC EAL5 assurance level. The Certification Report identifier is SERTIT-006 CR, issue 1.0, 1 November 2007 [9].

For the re-evaluation of Trusted Security Filter TSF101, the evaluators addressed every work unit 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. The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [8] to SERTIT, 23 March 2010. SERTIT then produced this Certification Report.

4.17 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

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.

5.1 Delivery

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

TOE is treated as CCI equipment, and is distributed according the Norwegian regulation for information security, Forskrift om informasjonssikkerhet [10] § 7-1 to § 7-45. The distribution is described in § 7-19.

5.2 Installation and Guidance Documentation

The developer performs all installation, generation, and start-up. The evaluators examined the guidance documents, TSF 101 Technical Manual [11] and the Software Installation guide [12] and determined that the steps necessary for secure installation, generation, and start-up are documented and that the procedures result in a secure configuration.

Furthermore all instructions and guidelines for the secure use of TOE are described in the TSF 101 Technical Manual [11]. No functions or interfaces are available to non-administrative users. Hence, specific user guidance for non-administrative users is not provided for the TOE.

A list of the guidance documents is given in annex A

5.3 Misuse

Administrators should follow the guidance [11] and [12] for the TOE in order to ensure that the TOE operates in a secure manner. The guidance documents adequately describe all possible modes 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 administer and use the TOE's security functions, and to detect insecure states.

To prevent possible misuse of the TSF 101 firewall it is recommended to inspect the audit log and the filter statistics periodically. Further information can be found in the TSF 101 Technical Manual [11].

5.4 Vulnerability Analysis

The evaluators found that each obvious vulnerability is described [13] 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 [14] was based on the visibility of the TOE given by the evaluation process.

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

5.5 Developer's Tests

The developer has thoroughly tested all security functions of the TOE and the tests are divided into four 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 TSF 101. Many of these tests include the security functions, which are implemented in hardware.
- Self tests – which are part of the implementation and are performed at start up and as supervision.
- System tests – which are performed on the actual version of both hardware and software.
- Integration tests – which are performed on the actual version of both hardware and software

172 tests are performed, and 46 of these tests are specified for the coverage of the security functions in TSF 101. These tests are part of both the system tests and integration tests.

5.6 Evaluators' Tests

5.6.1 Devised testing

The evaluation team decided to focus the testing on the error conditions in the following security functions for devised testing: SF.Security.Alarm,

SF.Information.Flow.Control, SF.Self.Test, SF.Fail.Secure, SF.Domain.Separation, SF:Firewall.Statistics and SF.Audit.Log.

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

The only security function that was not selected for devised testing is SF.Passive.Protection, which describes that the TOE has a physical sealing.

The evaluators performed 11 different tests.

5.6.2 Sample testing

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

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

The only security function that was not selected for testing is the SF.Passive.Protection, which describes that the TOE has a physical sealing.

The developer have specified 46 different tests for testing of the security functions in TSF 101, the amount of samples selected for testing by the evaluation team is 29 different tests, which is 63% of the developers testing effort.

The test configuration is described in annex A.

6 Evaluation Outcome

6.1 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 Trusted Security Filter TSF101 with hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ISC7, -ICS7A and -ISC7B and software version 3AQ 21850 CAAA Version 2.1.4 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.

6.2 Recommendations

Prospective consumers of Trusted Security Filter TSF101 with hardware versions 3AQ 21564 AAAA ICS5, -ICS5A, -ICS6, -ICS6A, -ICS6B, -ISC7, -ICS7A and -ISC7B and software version 3AQ 21850 CAAA Version 2.1.4 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 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.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Thales Trusted Security Filter TSF101 with

Software version:

- 3AQ 21850 CAAA Version 2.1.4

Hardware versions:

- 3AQ 21564 AAAA ICS5
- 3AQ 21564 AAAA ICS5A
- 3AQ 21564 AAAA ICS6
- 3AQ 21564 AAAA ICS6A
- 3AQ 21564 AAAA ICS6B
- 3AQ 21564 AAAA ISC7
- 3AQ 21564 AAAA ICS7A
- 3AQ 21564 AAAA ISC7B

TOE Documentation

The supporting guidance documents evaluated were:

- TSF101 Security Target [1]
- ACECom TSF Technical Manual [11]
- TSF101 Software Installation Guide [12]

TOE Configuration

The following configuration was used for testing:

The TSF 101 – Trusted Security Filter, consisting of hardware version 3AQ 21564 AAAA ICS7 and TSF 101 software version 3AQ 21850 CAAA Version 2.1.4.

The developer has provided a rationale on why the hardware versions listed above in "TOE Identification" are interchangeable. This rationale is also enclosed as Appendix A in the ETR [8].

During independent testing the developers test bed was used. This includes one PC with Windows XP Professional 2002 operating system and customized test software simulating the secure LAN. A similar PC was simulating the non-secure LAN, with customized test software for receiving messages from the secure LAN.

The following test software was used:

- MSIFCsim2 (3AQ 21852) ver. 2.1
- UDPListen2 (3AQ 21853) ver. 2.1

For penetration testing of the TSF 101 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

The definitions of the components used during evaluation/testing are:

MSIFC PC (Secure):	Type:	Dell Latitude D820
	Hardware:	Intel Core 2 CPU, 1,66 GHz, 1,99 GB RAM
	OS:	Windows XP Professional 2002, Service Pack 3
	SW:	ATOD message generator MSIFCsim2 ver. 2.1 (3AQ 21852 CAAA)
HCR/NAV PC (Non-secure):	Type:	Dell Latitude D820
	Hardware:	Intel Core 2 CPU, 1,66 GHz, 1,99 GB RAM
	OS:	Windows XP Professional 2002, Service Pack 2
	SW:	UDPListen2 ver. 2.1 (3AQ 21853 CAAA)
1 Ethernet network switch	Type:	Digital Data Communications FSW-0807TX Ver. 1A
1 Ethernet hub	Type:	Planet Tech Corp. Model EH500 (V.3)
1 Ethernet hub	Type:	Intel Business 5 port HUB
2 Media converters	Type:	Allied Telesyn International MC101XL Fast Ethernet media converter.

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

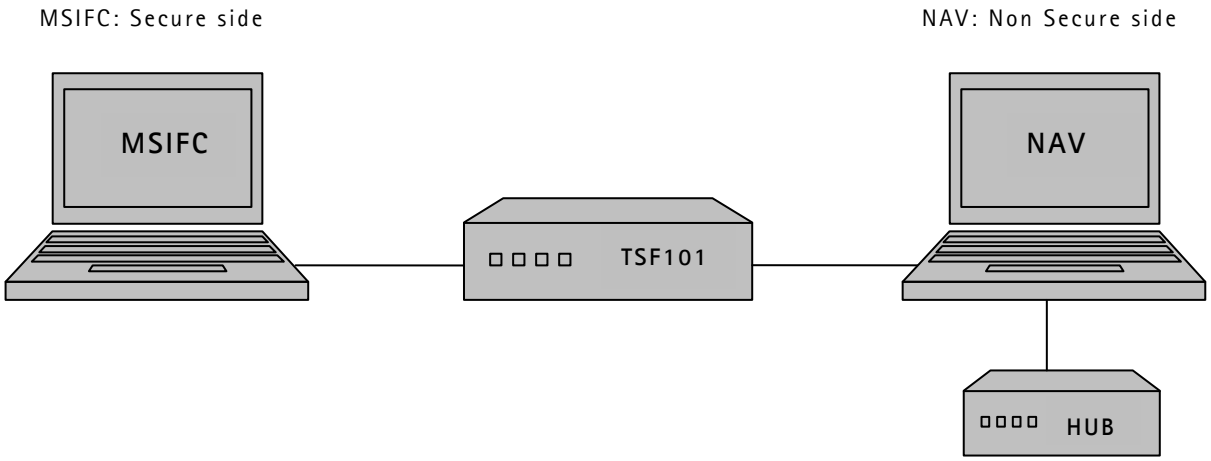


Figure 1 Test configuration MSIFC – NAV

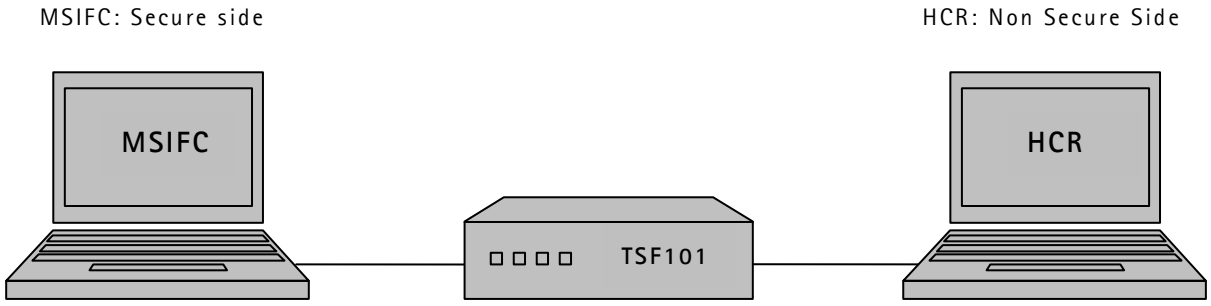


Figure 2 Test configuration MSIFC – HCR