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

SERTIT-019 CR Certification Report

Issue 1.0 16.09.2011

Special Processing Indicator Filter version 1.2

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

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

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

* Mutual Recognition under the CC recognition arrangement applies to EAL4

Contents

1 Certification Statement

The Special Processing Indicator Filter is a software based filter, designed and implemented to filter messages transferred between networks of different security domains.

Special Processing Indicator Filter version 1.2 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 EAL4 for the specified Common Criteria Part 2 conformant functionality for the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	16.09.2011

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
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
IAW	In Accordance With
KDA	Kongsberg Defense and Aerospace
MIDS	Multifunctional Information Distribution System
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPI	Special Processing Indicator
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Security Target for the SPI Filter, Pubic version 1.0, 09.08.2011.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report Common Criteria EAL4 Evaluation of Kongsberg Defence & Aerospace Special Processing Indicator Filter version 1.2, version 1.0, 2011-06-27.

[8] Air Defense Software Product SPI Filter Environment Computer Software Configuration Item (CSCI) Software Requirement Specification (SRS), SRS-60224895, Rev. A, 2011-05-09

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Special Processing Indicator Filter version 1.2 to the Sponsor, FLO Luftkapasiteter, 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* Special Processing Indicator Filter version 1.2.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Kongsberg Defence and Aerospace.

The Special Processing Indicator (SPI) filter is a software based filter, designed and implemented to filter messages transferred between networks of different security domains.

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

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 2.

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 EAL4 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in the ST[1], chapter 3.2

4.7 Security Claims

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

4.8 Threats Countered by the TOE

- Information Leaks by a hacker manipulating the system, or operator error, or information incorrectly crosses security domains
- The KDA- or system administrator misconfigures the filter, resulting in information incorrectly crossing security domains.
- Due to system failure the filter stops functioning and information incorrectly crosses security domains.
- Due to system failure, or setup configuration error, messages stopped by the system with SPI set to "on", are not audited.

4.9 Threats Countered by the TOE's environment

- A hacker manipulates the SPI bit of messages and information incorrectly crosses security domains.
- A hacker or an operator manipulates the audit trail to cover illegal actions.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- Security procedures for the TOE are established and in use.
- The TOE is used in the intended setup described in the ST[1], chapter 2.
- The SPI-filter is installed in an environment which either is manned, under surveillance, or placed in a protected location
- The developer has appropriate security measures installed and implemented to protect the TOE against tampering.
- KDA- and system administrators are competent to manage the TOE and the security of the information it contains and all operators know how to use the TOE in a secure manner.
- KDA- and system administrators and Operators are trusted not to misuse their authority.
- All personnel with access to the TOE, in the whole life-cycle of the TOE, hold the appropriate security clearance.
- The TOE and TOE environment shall not have any connections, directly or indirectly, to unclassified and/or public networks.

4.12 IT Security Objectives

- The TOE shall filter messages based on the SPI-bit when crossing the security domains:
  - from the originating domain to the receiving domains
- The TOE shall have the ability to audit all messages with:
  - SPI-bit set (and rejected to forward)
  - EMERGENCY or FORCE TELL and SPI-bit set
- The TOE shall give the operator an alarm if the audit trail is not writeable, or runs full.

4.13 Non-IT Security Objectives

- The system shall have a firewall installed filtering the IP based message traffic.
- There is a watchdog installed in the system. The operator gets an indication of system including SPI filter status from the watchdog. Green light indicates that the status is OK.
- The system has a restart button for the operator to re-establish normal operation after a system failure.
- System architecture and functionality ensures that it is not possible to bypass the filter. If the filter fails no messages are transmitted to the receiving security domain.
- The environment of the TOE shall be secured according to defence requirements, and prevent hackers to get access to TOE connected systems and communication lines.
- The developer environment shall be secure in a way that prevents hacker access of any kind.
- The operators, KDA- and system administrators of the systems shall be trained to securely operate and manage the systems.
- The KDA- and system administrators of the system shall be properly authenticated.
- The audit trail is protected by access control mechanisms in MMI workstation operating system (Solaris /Linux).
- The system administrator of the systems shall regularly, according to the security procedures, analyze the audit records.
- The operators, KDA- and system administrators of the systems shall hold an appropriate security clearance of at least "HEMMELIG".

4.14 Security Functional Requirements

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

- Complete information flow control (FDP_IFC.2)
- Simple security attributes (FDP_IFF.1)
- Audit data generation (FAU_GEN.1)
- Prevention of audit data loss (FAU_STG.4)

The full description of the SFRs can be found in the ST, chapter 6.1.

4.15 Security Function Policy

Tracks with SPI bit set shall only be shared between the originating network and respectively network.

Non-SPI track can be disseminated freely between networks IAW defined application filters.

Each message received to the filter is inspected. If the SPI-bit is set, the message is not forwarded.

The above approach has one exception:

> IAW MIL-STD 6016 and 6011/STANAG 5511, a track received with EMERGENCY or FORCE TELL indication, will pass all filters. In this case the tracks will be transmitted on all links, and the security audit trail shall reflect the transmittal. The SPI indication is retained on the transmitted track where applicable.

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 SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

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].

SERTIT monitored the evaluation which was carried out by the Norconsult AS Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT on the 27.06.2011. 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 4 assurance package.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

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

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] 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.

The EAL 4 evaluation of the Special Processing Indicator Filter has shown that it is methodically designed, tested and reviewed. The evaluation has further shown that the TOE is developed in a secure environment, uses well-defined development tools, has a properly defined life-cycle model and has procedures for standard commercial delivery services. The TOE is under proper configuration management, and follows strict procedures on how for instance changes to the TOE are reviewed and accepted. The guidance documentation helps implement the TOE into Systems in a secure manner. The TOE has been tested and reviewed for exploitable vulnerabilities using an Enhanced-Basic attack potential, by both the developer and evaluators.

If the TOE is not physically protected and managed as required for the highest level of security classified data handled by the TOE, the SPI Filter can be tampered with leading to the compromise of sensitive data or a denial of service caused by the disruption of the systems the SPI Filter is connected. During normal operations of the SPI Filter, does the environment restrict tampering of the Security Log File and the network layout ensures that all data which shall be SPI inspected are routed through the SPI Filter. Tests performed by the evaluator verify that SPI Filter does not forward messages in case of serious internal faults.

5.2 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.

5.3 Installation and Guidance Documentation

The SPI Filter is a software component designed to be an integrated part of an Air Defence System. The SPI Filter is by design not configurable, i.e. functionality such as generation of audit events is always on, and operates as a packet filter enforcing the SFP.

Since the SPI Filter is an integrated part of Air Defence Systems, and not a stand-alone product, the guidance documentation includes detailed description for how to compile and build the software component which is to be included. Assumptions that the SPI Filter requires to be satisfied by the environment are also unambiguously defined and a part of the SPI Filter guidance documentation. Installation and user guidance is not relevant for the TOE, since the TOE operates without user interference and system installation ensures that the SPI Filter is included into the Air Defence System environment in accordance with the SPI Filter environment requirements.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. However, this TOE is a software component designed to be an integrated part of an Air Defence System. The SPI Filter is by design not configurable, i.e. functionality such as generation of audit events is always on, and operates as a packet filter enforcing the SFP. The TOE operates without user interference and system installation ensures that the SPI Filter is included into the Air Defence System environment in accordance with the SPI Filter environment requirements.

5.5 Vulnerability Analysis

The evaluators' assessment of potential exploitable vulnerabilities in the TOE has been addressed and shows that the vulnerability analysis is complete, and that the TOE in its intended environment is resistant to attackers with an Enhanced-Basic attack potential.

5.6 Developer's Tests

The evaluators' assessments of the developers' tests shows that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements. The testing performed on the TOE by both the developer and evaluator showed that the EAL 4 assurance components requirements are fulfilled.

5.7 Evaluators' Tests

The evaluator have independently tested the TSFs and verified that the TOE behaves as specified in the design documentation and confidence in the developer's test results is gained by performing a sample of the developer's tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Special Processing Indicator Filter version 1.2 meets the Common Criteria Part 3 *conformant* requirements *of* Evaluation Assurance Level EAL4 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 Special Processing Indicator Filter version 1.2 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

The system where the SPI Filter is integrated consists of several computers dedicated to different function. The Sealed Area contains equipment and cabling that gives direct access to classified information. All personnel with access shall be authorised for this information and equipment.

Dedicated data links are used for communication with the environment outside the Sealed Area, via Crypto, Firewall or MIDS/L16 Terminal. No other external connection exists (e.g. IP via servers). No wireless devices exist.

Input to the filter is a message headed for the receiving security domain. The message is first inspected for SPI bit set to "on" or "off". If the SPI bit is "off" the send function is called, and the message is send. Else if the SPI bit is set to "on", i.e. this message is by the main rule not to leave the system, an event is registered in the security audit trail, and the message is further inspected for any EMERGENCY or FORCE TELL indicator. If there is no such indicator present, the message is stopped. Else if an indicator is present the send function is called and the message is sent.

The audit events are written to an audit trail that is stored in one of the MMI computers and protected by the access control mechanisms in the MMI workstation operating system (Solaris/Linux). If it is not possible to write to the audit trail, an alarm is given. If the audit trail runs full, the oldest stored events are overwritten, and an alarm is given to the operator.

TOE Documentation

The supporting guidance documents evaluated were:

[a] Air Defense Software Product Software Product Specification (SPS) for the SPI Filter SW (SPS-60221138) Rev. A 2011-05-05

[b] Air Defense Software Product Software Version Description (SVD) SPI Filter Software CSCI (SVD-60221138) Rev. A 2011-05-09

[c] KDA SPI Filter Software Development Plan (SDP-60220685) Rev. D 2011-05-05

[d] Air Defense Software Product SPI Filter Environment Computer Software Configuration Item (CSCI) Software Requirement Specification (SRS), SRS-60224895, Rev. A, 2011-05-09

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

TOE Configuration

The following configuration was used for testing:

- SPI Filter Software Component version 1.2.
- The SPI Filter is a software component which is installed on a Real Time (RT) Computer with PowerPC CPU and VxWorks 5.5.1 Operating System.

- The security audit trail is stored on the hard drive of one of the MMI workstations, operating system: Solaris/Linux.