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

SERTIT-013 CR Certification Report

Issue 1.0 28 June 2011

GL1 Computer Software Component of SkyView 2.0.9-i2

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 judgments 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 judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

Contents

1 Certification Statement

The TOE is GL1 Computer Software Component of SkyView. SkyView is the C2 application of NORGIL. NORGIL is the Norwegian Ground Infrastructure for Link 16. GL1 is filtering messages in the system.

GL1 Computer Software Component of SkyView version 2.0.9-i2 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 4 for the Common Criteria Part 2 conformant functionality when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier Arne H. Rage
Quality Assurance	Lars Borgos Quality Assurance Lars Borgos
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	28 June 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
OSP	Organizational Security Policy
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy

3 References

[1] SkyView Link1 Interface Security Target, 3AQ 23805 AAAA SC Rev. D, 10.05.2011

[2] Common Criteria Part 1, CCMB-2006-09-001, Version 3.1 R1, September 2006.

[3] Common Criteria Part 2, CCMB-2007-09-002, Version 3.1 R2, September 2007.

[4] Common Criteria Part 3, CCMB-2007-09-003, Version 3.1 R2, September 2007.

[5] Om sertifiseringsordningen, SD001, Versjon 8.0, 18.02.2011.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2007-09-004, Version 3.1 R2, September 2007.

[7] Evaluation Technical Report, Common Criteria EAL4 Evaluation of GL1 Computer Software Component of SkyView, TOE version 2.0.9-i2. S-2402/20.06 version 1.1, 23.05.2011

[8] SkyView Installation, configuration and maintenance manual FAHF1 61118243-354 CSOM Rev A 2009-10-29

[9] Common Criteria Assurance Class ALC Compliancy Document Assurance Class ALC rev A2

[10] CDRL 30 Configuration Management Plan CMP TNOR NORGIL CMP rev D

[11] SkyView VDD for Build C 61118243_498_revAC_VDD_SKYVIEW_buildC

[12] FAAT for the Link 1 SPI filter, Minutes of Meeting 3AQ 23800 AAAA VE 2010-01-19

[13] SkyView Link 1 SPI Filter Software Design Document, Link 1 SPI Filter SDD Rev B

[14] Common Criteria Assurance Class AGD Compliancy Document, Assurance Class AGD rev B

[15] ARCADES Control HMI ARCADES Data Reduction HMI Software User Manual, FAHF1 61118243-108 SUM ARCADES Rev A – 20091204

[16] SkyView Operational HMI Software User Manual, FAHF1 61118243-108 SUM VISU Rev C – 20100601

[17] STANAG 5516 Ed 3

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of GL1 Computer Software Component of SkyView version 2.0.9-i2 to the Sponsor, FLO/I, 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 GL1 Computer Software Component of SkyView and version 2.0.9-i2.

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 TOE is the GL1 Computer Software Component of SkyView. SkyView is a component of MASE Interface Units (MIU), which in turn is a component of NORGIL. SkyView is the NORGIL C2 (Command and control) application, processing radar inputs, Link 1 and Link 16 messages.

GL1 shall ensure that it transmits only Link 1 formatted messages to the Link 1 interfaces.

GL1 shall prevent air tracks protected by the SPI (Special Processing Indicator) to be transmitted on Link 1 interfaces, unless authorized by Emergency indicator or Force Tell indicator.

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 4 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 is compliant with the policy for handling SPI protected information as outlined in STANAG 5516 Ed 3 [17].

The description of the OSP is as follows: "An air track shall not be transmitted on Link 1 when a source is marking this track with SPI = 1, unless the track is marked as Emergency or Force Tell".

4.7 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats and OSP's 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.

4.8 Threats Countered

A TOE user (TA.USER) may release SPI protected tracks (AS.NS) to systems operating at lower security level without authorization.

4.9 Threats Countered by the TOE's environment

No threats countered by the environment are described.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The processing resources of the TOE are assumed to be located within controlled access facilities that will prevent unauthorized physical access.

4.12 IT Security Objectives

The IT security Objectives are:

O.AUDIT	The TOE will initiate recording of security relevant events, to assist a security officer in the detection of potential violations of the security policy for protection of SPI protected information.
O.SPI_L1_FILTER	The TOE will prevent information to be transmitted to Link 1 according to P.SPI_L1 policy.

4.13 Non-IT Security Objectives

The non-IT Security Objectives are:

OE.ACCESS	The TOE environment will provide the means of controlling and limiting access to the TOE IT environment to authorized users.
OE.AUDIT	The TOE environment will provide the means of recording security relevant events, so as to assist a security officer in the detection of potential violations of the security policy for protection of SPI protected information, and also to hold users accountable for any actions they perform that are relevant to this security policy.
OE.AUDITLOG	Administrators of the TOE must ensure that audit facilities are used and managed effectively. In particular: a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space. b) Audit logs should be inspected on a regular basis, and appropriate action should be taken on the detection of breaches of security.
OE.L1_CHANNEL	The TOE environment will provide the means to ensure that only messages from the TOE are transmitted on Link 1 interfaces.
OE.OS	The operating system will provide process isolation capability including isolation of data with respect to any other process running on the same computer.
OE.PHYSICAL	Those responsible for the TOE and its IT environment must ensure that the hardware components of the IT environment is protected from physical attack which might compromise IT security, and that the physical protection for the hardware components is sufficient for protection of the information handled by the hardware components.

4.14 Security Functional Requirements

The TOE provides security functions to satisfy the following SFRs:

FAU_GEN.1	Audit data generation
FDP_ETC.1	Export of user data without security attributes
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FPT_STM.1	Reliable time stamps

4.15 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 Secode Norge AS Information Technology Security Evaluation Facility (ITSEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT in 23.05.2011. SERTIT then produced this Certification Report.

4.16 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 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.

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.

The delivery documentation [8], [9], [10], [11] and [12] describes all procedures used to maintain security of the TOE when distributing the TOE to the user.

5.3 Installation and Guidance Documentation

The ST [1], and the guidance documents [13], [14], [15] and [16] describes the procedures necessary for the secure installation of the TOE and the secure preparation of the operational environment are in accordance to the ST.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Administrators should follow the guidance [13], [14], [15] and [16] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode 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.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluators devised 3 penetration tests based on the independent search for potential vulnerabilities. These tests cover all items in the vulnerability analysis.

5.6 Developer's Tests

The developer has thoroughly tested all security functions of the TOE and the tests are divided in the following test case parts:

- SPI filtering & recording, track inside Link 1 Track Continuity Area (TCA)
    - SF.SPI_Filter
    - SF.Link1_Enc
    - SF.Audit
- SPI filtering & recording, track outside Link 1 Track Continuity Area (TCA)
    - SF.SPI_Filter
    - SF.Link1_Enc
    - SF.Audit

The number of tests performed by the developer is 28.

5.7 Evaluators' Tests

The evaluation team decided to perform the devised testing on all 3 TSFs and on 7 of the TSFIs:

- SF.SPI_FILTER
- SF.Link1_ENC
- SF.AUDIT

TSFI external to GL1

- SYE
- SYR
- ACD

TSFI internal in GL1 (to/from TSF)

- SF.SPI_Filter -> Link1_Mgmt
- SF.SPI_Filter -> SF.Audit
- Link1_Mgmt -> SF.Link1_Enc
- SF.Link1_Enc -> SF.Audit

The TSFI Link1_Dec -> SF.Audit was tested during sample testing. The Link 1 decoding has no security functionality.

The evaluators devised and performed 8 tests.

The evaluators have tested a sample of 28 (all) tests of the developer's tests and verified expected and actual results.

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 GL1 Computer Software Component of SkyView version 2.0.9-i2 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 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 GL1 Computer Software Component of SkyView version 2.0.9-i2 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:

GL1 Computer Software Component of SkyView (TOE version 2.0.9-i2)

TOE Documentation

The supporting guidance documents evaluated were [13], [14], [15] and [16] in the references list.

TOE Configuration

The following configuration was used for testing:

The GL1 Computer Software Component of SkyView test environment is fully distributed. GL1 Computer Software Component (TOE) is installed on (SkyView) HP Server, with HP-UX 11i v1 (OS English).