Certification Report

EAL 4+ Evaluation of Luna® CA4 System Version 2.6

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-114-CR
Version: 1.0
Date: 23 February 2012
Pagination: i to iii, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada, located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 23 February 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- Luna®, which is a registered trademark of SafeNet, Inc.

TABLE OF CONTENTS

Executive Summary

Luna® CA4 System Version 2.6 (hereafter referred to as Luna® CA4 System), from SafeNet, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

Luna® CA4 System is a host-attached hardware cryptographic module or Hardware Security Module (HSM).

The Luna® CA4 System provides a component for the performance of cryptographic functions for key generation, key storage, encryption and decryption, digital signature and verification used by application systems that provide cryptographic support functions such as a Certificate Authority/Certification Service Provider (CA/CSP) or Time Stamp Authority (TSA). The Luna® CA4 System includes processors, read-only and random-access memory, and firmware along with Cryptographic Application Programming Interface (API) software that resides on the host computer. The Luna® CA4 System incorporates FIPS 140-2 validated cryptography.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 20 January 2012 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Luna® CA4 System, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.2 - Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Luna® CA4 System evaluation meets all the conditions of the *Arrangement on the*

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Recognition of Common Criteria Certificates and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented, evaluation is Luna® CA4 System Version 2.6 (hereafter referred to as Luna® CA4 System), from SafeNet, Inc.

2 TOE Description

The Luna® CA4 System is a host-attached hardware cryptographic module or Hardware Security Module (HSM).

The Luna® CA4 System provides a component for the performance of cryptographic functions for key generation, key storage, encryption and decryption, digital signature and verification used by application systems that provide cryptographic support functions such as a Certificate Authority/Certification Service Provider (CA/CSP) or Time Stamp Authority (TSA). The Luna® CA4 System includes processors, read-only and random-access memory, and firmware along with the Cryptographic Application Programming Interface (API) software that resides on the host computer. The Luna® CA4 System incorporates FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Luna® CA4 System is identified in Section 6 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
Luna® CA4 (Level 3 Validation)	*Pending* [2]

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Luna® CA4 System:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	1785
Triple Data Encryption Standard (Triple-DES)	ANSI X9.52-1998 in conjunction with FIPS 46-3	1157

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

Cryptographic Algorithm	Standard	Certificate #
Secure Hash Standard (SHS)	FIPS 180-3	1567
Digital Signature Algorithm (DSA)	FIPS186-2 and FIPS186-3	561
Rivest, Shamir, Alderman (RSA)	FIPS186-2 and FIPS186-3	892
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS186-2 and FIPS186-3	241
Hash Based Message Authentication Code (HMAC)	FIPS 198	1050
Triple DES Message Authentication Code (Triple-DES MAC)	FIPS 113	Triple-DES Cert. #1157, vendor affirmed
Random Number Generator (RNG)	ANSI X9.31	947
Key Agreement Scheme (KAS)	SP 800 56A	24
Key Definition Function (KDF)	SP 800-108	SP 800-108, vendor affirmed

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Security Target for Luna® CA4 System Version 2.6
Version: 7
Date: December 20, 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Luna® CA4 System is:

a. Common Criteria Part 2 extended, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirement defined in the ST;
   - FDP_BKP.1 – Backup and Restoration.

b. Common Criteria Part 3 conformant, with security assurance requirements based only on assurance components in Part 3;
c. Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

The Luna® CA4 System provides security management functions by giving the Security Officer the ability to establish the policy that will govern the cryptographic module's operation, according to the requirements of the customer organization, by enabling/disabling or refining the corresponding policy elements to equate to or to be more restrictive than the pre-assigned capabilities. Details of these security policies can be found in Section 1.4 of the ST, and in the Luna® CA4 Security Policy document.

In addition, the Luna® CA4 System implements policies pertaining to identification and authentication, security management, protection of TOE security functions, trusted path, and resource utilization. Further details on these security policies may be found in Sections 6 and 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Luna® CA4 System should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- A competent authority will be assigned to manage the Luna® CA4 System and the security of the information that it contains and who can be trusted not to deliberately abuse their privileges so as to undermine security. She/he is, however, capable of error;

- A competent authority within the Luna® CA4 System environment reviews the raw data generated and exported by the Luna® CA4 System to generate any audit records required by the policy in place in the environment;

- The data submitted to the Luna® CA4 System by the host application is assumed to be correct;

- The host application will provide an interface and communication path between human users and the Luna® CA4 System because the Luna® CA4 System does not have a human interface for authentication and management services;

- Firmware update packages are digitally signed by the vendor using a private key whose use is restricted to this purpose and the digital signature is verifiable by an instance of the Luna® CA4 System;

- The host application software is assumed to be operating as the Luna® CA4 System user on behalf of a human user. As such, any direct interaction with the Luna® CA4 System, including authentication, is performed by the host application as the user of the Luna® CA4 System; and

- The Luna® CA4 System will not, in general, be aware of the identities of end-users authorized for the Luna CA4 System services. It is assumed that the management of the individual user assignments for the three Luna® CA4 System roles is done in the environment in a trustworthy fashion according to a well-defined policy.

7.2 Environmental Assumptions

The following Environmental Assumption(s) are listed in the ST:

- The TOE environment ensures the availability of the backup data; and

- When in operation and when stored as a backup, the TOE is assumed to be located within a controlled access facility providing physical security that is adequate to prevent physical access by unauthorized persons.

7.3 Clarification of Scope

The Luna® CA4 System does provide physical and logical countermeasures to counter attempts by unauthorised users to compromise token data. However, the token does not counter threats related to deliberate, compromising actions performed by an authorised local user.

8 Evaluated Configuration

The Luna® CA4 System Security Target defines the system components in the evaluated configuration. The Luna® CA4 System consists of the following components:

- two (2) SafeNet, Inc. Luna® CA4 devices, each in a PC Card form factor, (referred to as tokens) (Hardware Versions 808-000014-002 [900578-001] and 808-000003-001 [900578-002]; Firmware Version 4.8.7);

- a dual-slot Luna® Dock II PC Card Reader (Hardware Version 908-55007-001 [006850-001]; Firmware Version 0x00C1);

- Luna® PIN Entry Device (PED II) (Hardware Versions 908-25024-001 and 908-000008-002 [808-00012-002]; Firmware Versions 2.0.2 and 2.4.0) and iKeys with labels;
- lunacm (setup and administration) software (Version 2.3.3); and
- Luna® CA4 software, version 2.6.

A Quick Start Guide for Luna® CA4 Release 2.6 describes the procedures for secure initialization of the product. A Content Sheet identifies the Luna® CA4 System components that the customer should expect to find in the delivered product.

9 Documentation

The SafeNet documents provided to the consumer are as follows:

- Quick Start Guide for Luna® CA4 Release 2.6;
- The Online Help system provides the detailed Administrator/User guidance for the operation of the product;
- Luna® CA4 Release 2.6 release notes; and
- Update Sheet, Luna PCM/CA4 SW v2.6 FW 4.8.7, document number 007-011134-002.

Note - Guidance documents provided with the Luna® CA4 System are primarily intended as Administrator guidance. The administration functions are normally carried out by the Security Officer, or possibly a designated User, using the CLI software as the interface. In most cases, these functions will be performed very infrequently.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Luna® CA4 System, including the following areas:

Development: The evaluators analyzed the Luna® CA4 System functional specification, design documentation, and a subset of the implementation representation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Luna® CA4 System security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Luna® CA4 System preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the Luna® CA4 System configuration management system and associated documentation was performed. The evaluators found that the Luna® CA4 System configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Luna® CA4 System during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Luna® CA4 System design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by SafeNet for Luna® CA4 System. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Luna® CA4 System. Additionally, the evaluators conducted a review of public domain vulnerability databases, a focused search of all evaluation deliverables, and a review of publicly available papers describing potential attacks against HSMs. Some potential vulnerabilities were postulated; however in every case the calculated attack potential was significantly higher than the Enhanced-Basic level identified in the ST.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of EWA-Canada test goals:

- Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests to gain a better understanding of the TOE;

- Identification and Authentication: The objective of this test goal is to ensure that the TOE's User Identification and Authentication functional requirements have been met;

- Security Management: The objective of this goal is to demonstrate that the TOE's Security Data Management and Security Function Management functional requirements have been met;

- Access Control: The objective of this goal is to demonstrate the TOE is correctly enforcing its prescribed identity-based access control policy;

- Backup & Recovery: The objectives of this goal are twofold:

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

- demonstrate that the TOE maintains its secure state in the event of a failure and resume operation as described in the ST; and
- demonstrate that the TOE provides the authorized user with the ability to:
  - back-up user partition objects to another HSM, or (as determined by the user) and;
  - back-up user partition objects to an encrypted file on the host computer and recover the encrypted objects into the same or different HSM at a later time.

- Data Authentication: The objective of this test goal is to demonstrate that the TOE provides the two data authentication mechanisms specified in the ST;
- Integrity Check: The objective of this test goal is to ensure that the requirements associated with TSF *Logical Self-Protection of Security Functions* are met;
- Token Cloning / Backup: The objective of this test goal is to demonstrate TOE compliance with the following TSFs: *Access Control*, *Backup and Recovery*, *Cloning*, *Key Export and Import Protection*, *Multi-Session Capability*, and *Object Reuse*. Test cases will be prepared to demonstrate that the TOE:
  - maintains its secure state in the event of a failure and resume operation as described in the ST; and
  - provides the authorized user with the ability to clone tokens and user partitions to another HSM.
- Failure Handling: The objective of this test goal is to use and confirm the ability of the TOE to handle failures consistent with the TSFs for *Failure Handling* and *Preservation of Secure State;*
- Split Knowledge TOE Access: The objective of this test goal is to demonstrate that the following TSFs that contribute to the TOE's split knowledge access control mechanism (M of N) are met:
  - *M of N Activation*;
  - *User Identification & Authentication;*
  - *Trusted Path - Luna PED II;*
  - *HSM Level Capabilities*; and
  - *Security Function Management.*

11.3 Independent Penetration Testing

Based on the vulnerability assessment (section 10), which had demonstrated that the TOE is resistant to an attacker with enhanced-basic attack potential, the evaluation facility did not

levy any additional penetration tests against the TOE beyond those already performed by the developer.

11.4 Conduct of Testing

Luna® CA4 System was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Luna® CA4 System behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for the Luna® CA4 System includes a comprehensive Installation and Security Guide and a Users Guide.

The Luna® CA4 System is straightforward to configure, use and integrate into a corporate network.

Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certificate Authority
CA/CSP	Certificate Authority/Certification Service Provider

Acronym/Abbreviation/ Initialization	Description
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CPL	Certified Products list
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HMAC	Hash-Based Message Authentication Code
HSM	Hardware Security Module
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
KAS	Key Agreement Scheme
KDF	Key Definition Function
NIST	National Institute of Standards and Technology
PALCAN	Program for the Accreditation of Laboratories - Canada
PCMCIA	Personal Computer Memory Card International Association
PED	PIN Entry Device
PIN	Personal Identification Number
QA	Quality Assurance
RNG	Random Number Generator
RSA	Rivest, Shamir, Aldeman
SFR	Security Functional Requirement
SHS	Secure Hash Standard
ST	Security Target
TOE	Target of Evaluation
Triple DES	Triple Data Encryption Algorithm
Triple DES MAC	Triple DES Message Authentication Code
TSA	Time Stamp Authority
TSF	TOE Security Functions

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Security Target for Luna® CA4 System Version 2.6, Version 7, December 20, 2011 .

e. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of SafeNet, Inc. Luna® CA4 System Version 2.6, Document No. 1619-000-D002, Version 1.0, 20 January 2012.