Certification Report

EAL 4+ Evaluation of Chrysalis-ITS, Inc.

Luna® CA³

Version 3.97, Software Versions 8.0 and 8.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-13
Version: 1
Date: 22 November 2002
Pagination: i to iv, 1 to 14

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and 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 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*. This certification report, and associated certificate, applies only to the specific 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 associated certificate, is not an endorsement of the IT product by the Communications Security Establishment (CSE) or by any other organization that recognizes or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and 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. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, managed by the Communications Security Establishment.

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the CCS Certification Body for approval to perform Common Criteria evaluations. A significant requirement for such approval is accreditation to the requirements of the *ISO Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates–Canada, Limited, located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that a product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines and scopes 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 (evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22 November 2002, 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 Canadian certified products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html
This certification report makes reference to the following trademarked names: Microsoft® Windows NT® and Windows 2000®, which are registered trademarks of Microsoft Corporation; Solaris®, which is a registered trademark of Sun Microsystems Corporation; and Luna®, which is a registered trademark of Chrysalis-ITS, Inc.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Luna® CA³, Version 3.97, Software Versions 8.0 and 8.1, from Chrysalis-ITS, Inc., is the Target of Evaluation (TOE) for this EAL 4 augmented evaluation. The Luna® CA³ provides the cryptographic processing required for a Public Key Infrastructure (PKI). Within a PKI, the Certificate Authority (CA) is the most trusted component and is responsible for signing public key certificates and Certificate Revocation Lists (CRLs). The certificates and CRLs ensure the integrity and authenticity of private and public keys. The CA's private signature key forms the basis for all trust of the PKI and must be afforded the maximum protection possible.

The Luna® CA³ performs different types of cryptography and has been awarded a FIPS 140-1 Security Level 3 validation (FIPS 140-1 Certificate #214) under the Cryptographic Module Validation Program.

The Luna® CA³ counters threats against the:

1. Confidentiality and integrity of user key material – private keys and secret keys;
2. Confidentiality, integrity and authenticity of user data;
3. Confidentiality of user authentication data;
4. Access to cryptographic functions;
5. Integrity of security functions;
6. Confidentiality and integrity of security function data; and
7. Integrity of the cryptographic material management process.

Electronic Warfare Associates–Canada (EWA-Canada) is the Common Criteria evaluation facility that conducted the evaluation. The evaluation was completed on 6 November 2002, 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 (ST), which identifies assumptions made during the evaluation, the intended environment for the Luna® CA³, the security requirements, and the level of confidence (evaluation assurance level) that the product satisfies the security requirements. Consumers of the Luna® CA³ are advised to verify that their own environment is consistent with the environment identified in the ST, and to give due consideration to the comments, observations and recommendations in this Certification Report (CR).

The results documented in the Evaluation Technical Report[1] for this product indicate that the product meets the EAL 4 augmented assurance requirements for the evaluated security

[1] The Evaluation Technical Report contains company proprietary information and as such is not publicly releasable.

functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*. The Luna® CA³ Version 3.97 is conformant with:

1. Common Criteria Part 2 extended, containing security functional requirements from Part 2 and one extended security functional requirement: FDP_LUNA_BKP.1 (Luna Backup); and
2. Common Criteria Part 3 EAL 4 augmented, containing security assurance requirements from the EAL 4 package defined in Part 3, and one additional Part 3 security assurance requirement: ALC_FLR.2 (Flaw Reporting Procedures).

The Communications Security Establishment, as the CCS Certification Body (CB), declares that the Luna® CA³ Version 3.97, Software Versions 8.0 and 8.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the Certified Products List.

1 Identification of Target of Evaluation

The scope of this evaluation is the Luna® CA³, Version 3.97, Software Versions 8.0 and 8.1, cryptographic hardware security module. The Luna® CA³ evaluated platform is supported for: Microsoft® Windows NT® Version 4 (SP 5 or SP 6), Microsoft® Windows® 2000, and Sun Microsystems Solaris® 2.7 and 2.8. All other components referred to in this document, though typically present in a deployment, are not covered by this evaluation and certification (e.g., the host computer and operating system).

2 Product Description

The Luna® CA³, Version 3.97, Software Versions 8.0 and 8.1, provides a physically and logically protected component for the performance of cryptographic functions for key generation, key material storage and disposal, encryption and decryption, digital signature, and verification. The Luna® CA³ includes a processor, FLASH and random-access memory, and firmware packaged in a tamper-resistant form along with a small amount of host platform-specific communications support software.

The boundary of the Target of Evaluation (TOE), see Figure 1, includes:

1. Two identically configured printed circuit boards embedded in tamper-resistant Type II PC Card carrier packages, known as Luna® CA³ tokens. Each PC Card package hosts volatile and non-volatile memory, a microprocessor with associated firmware, data, control and key transfer signal paths, an input/output controller, power management, and a local oscillator.
2. A specially constructed dual PC Card reader, known as the Luna® Dock.
3. The PIN Entry Device (PED), which is housed in a separate physical enclosure and, through a physically and electrically separate data port connection to the token, provides a trusted path for the entry of plaintext critical security parameters (authentication data and cryptographic parameters) to the token.
4. PED Keys, which are serial memory devices used to store critical security parameters for entry through the PED.
5. Enabler software, which provides the human user with an interface on the host computer for initial product configuration and maintenance functions.
6. A Public Key Cryptography Standard (PKCS) #11-compliant cryptographic API, implemented as a Windows DLL or UNIX SO library (depending on the host platform configuration), which provides the PKCS #11 interface to a host software application acting on behalf of the human user of the Luna® CA³.

Figure 1 - Luna® CA³ Product

The Luna® CA³ provides cryptographic functions to meet the security requirements specified in the Security Target (ST). The Luna® CA³ is connected to a computer system, and provides the cryptographic operations requested by the applications running on that system. The applications use the PKCS #11 standard to communicate with the Luna® CA³. The Luna® CA^3 provides cryptographic material management and cryptographic operations using key data that is secured in the token.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Luna® CA³ is identified in section 5.1 of the Security Target.

The following Government of Canada approved algorithms were evaluated for correct implementation in the Luna® CA^3: DES, Triple-DES, DES MAC, Triple-DES MAC, DSA, SHA-1, Diffie-Hellman, RSA, and CAST5. As part of this effort, the evaluator made use of results generated under the Cryptographic Module Validation Program (CMVP), as follows:

The Luna® CA³ has been validated to FIPS 140-1 Security Level 3 (FIPS 140-1 Certificate #214) under the CMVP. Cryptographic algorithms tested under the CMVP are:

1. Data Encryption Standard (DES), FIPS 46-3 Certificate #32;
2. Triple-DES, FIPS 46-3 Certificate #32;
3. Digital Signature Algorithm (DSA), FIPS 186-2 Certificate #13; and
4. Secure Hash Algorithm (SHA-1), FIPS 180-1 Certificate #64.

The following algorithms were explicitly tested as part of this evaluation, with assistance provided by CSE: SHA-1, CAST5, and RSA.

The Luna® CA^3 also includes the following algorithms that were outside of scope of evaluation, and were not tested: RC, RC2, RC4, CAST, CAST3, CAST MAC, CAST3 MAC, CAST5 MAC, MD2, MD5.

4 Security Target

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

Security Target for Luna® CA^3 Version 3.97
Change Level: 12
Change Date: 1 November 2002
Document Number: CR-0246

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1,* with the final interpretations listed in Section 16. The Luna® CA³ Version 3.97 is conformant with:

1. Common Criteria Part 2 extended, containing security functional requirements from Part 2 and one extended security functional requirement: FDP_LUNA_BKP.1 (Luna Backup); and
2. Common Criteria Part 3 EAL 4 augmented, containing the security assurance requirements from the EAL 4 package defined in Part 3, and one additional Part 3 security assurance requirement: ALC_FLR.2 (Flaw Reporting Procedures).

6 Security Policy

This section is intended to provide a description of the policies that the TOE is required to enforce.

6.1 Token Access Control Policy

The token access control policy, which is set via policy vectors, governs the creation, storage, handling, and destruction of all objects in the TOE.

6.2 Identification and Authentication policy

The Luna® CA^3 token's identification and authentication policy defines three user roles: public user, token user, and security officer. A user's role is one of the key elements in access control decisions.

6.3 Hardware Security Policy

The hardware security policy requires that the Luna® CA^3 token hardware be constructed in such a way that physical tampering is evident through visual inspection

6.4 Firmware Security Policy

The firmware security policy assumes that any firmware images loaded in conformance with the policy have been verified by Chrysalis-ITS to ensure that the firmware will function correctly. The policy requires that only properly formatted firmware be loaded, and applies to initial firmware loading and subsequent firmware updates.

6.5 Fault tolerance policy

The TOE, in support of all policies, will remain in a secure state in the event of any type of failure.

6.6 Backup and Recovery Policy

The Luna® CA^3 shall provide the capability to securely backup a token by the security officer or token user. The token shall maintain its secure state and permit recovery of operations as described below:

1. In the event of host system discontinuity, the token shall allow recovery to its last operational state when the host system restarts.
2. In the event that power to the token is lost, it shall maintain its secure state and require the security officer or token user to login prior to resuming operation. The token shall resume operation with all security properties intact, but the operational state of the token prior to loss of power will be lost.
3. Recovery is permitted in the event of token failure or catastrophic damage to the token; it is performed by inserting and activating a backup token.

7 Assumptions and Clarification of Scope

7.1 Secure Usage Assumptions

For purposes of this evaluation, the Luna® CA³ security officers are assumed to be trusted and to understand the correct usage of the token. The Luna® CA³ system should be installed and configured using the guidance specified in the *Luna® PKI HSM Installation Guide* – Document No. 800193-000 Rev. A, and in the *Luna® PKI HSM Planning and Integration Guide* - Document No. 800194-000 Rev. A. The product should only be operated in the intended operating environment as specified in the ST and the guidance documentation.

7.2 Environmental Assumptions

There are a number of assumptions made about the operating environment of the TOE and they are as follows:

- The Luna® CA³ operates in an environment that is assumed to be physically secure, and all connection points to the TOE and the host computer are assumed to be contained within the physically secure environment.
- The environment is assumed to have adequate protection against power interruption and protection from disasters such as fire and flood.
- It is assumed that there is adequate protection from strong electromagnetic radiation and protection from unauthorized disclosure of data due to electromagnetic radiations from the TOE.
- It is assumed that only legitimate applications in the host IT environment will have access to the token.

For more information about the assumptions on the TOE security environment, see Section 3 of the ST.

Some of the secure usage assumptions about the operating environment, including the physical security requirements and separation of duties, were relaxed to facilitate the testing of the Luna® CA³ at EWA-Canada.

7.3 Clarification of Scope

The TOE does provide physical and logical countermeasures to ensure that unauthorised users cannot compromise token data. However, the token does not counter threats related to deliberate, compromising actions performed by an authorised local user.

8 Architectural Information

The Luna® CA³ system is comprised of the following six architectural layers:

1. The *hardware layer* provides the security functions and the physical electrical connections between different physical components of the Luna® CA³;
2. The *socket services layer* provides a software interface to the hardware layer as defined in the PC Card standard;
3. The *card services layer* provides central resource management for client software;
4. The *driver layer* (for each supported operating system) provides a connection between the host operating system and the Luna® CA³;
5. The *Cryptoki layer* is an implementation of the PKCS #11 standard; and
6. The *application layer* is where the applications requiring cryptographic services reside.

9 Evaluated Configuration

The evaluated version of the TOE is the Luna® CA³, Version 3.97, Software Versions 8.0 and 8.1, cryptographic hardware security module. In the evaluated configuration, the TOE may be used with Microsoft® Windows NT® Version 4 (Service Pack 5 or 6), Microsoft® Windows® 2000, and Sun Microsystems Solaris® 2.7 and 2.8 operating system platforms.

10 Documentation

The existing guidance documentation for the Luna® CA³ is:

1. Luna® PKI Enterprise Systems - Installation Guide - 800122-003 (for Version 8.0),
2. Luna® PKI Enterprise Systems - User Guide – 800123-002 (for Version 8.0),
3. Luna® HSM Installation Guide - 800193-000 (for Version 8.1), and
4. Luna® HSM Planning and Integration Guide – 800194-000 (for Version 8.1).

As a result of this evaluation, both sets of documents have been combined into one set of guidance documents supporting both software versions 8.0 and 8.1:

1. Luna® PKI HSM Installation Guide - 800193-000 Rev. A, and
2. Luna® PKI HSM Planning and Integration Guide – 800194-000 Rev. A.

11 Evaluation Analysis Activities

The evaluation involved an analysis of the developer's processes for developing and supporting the Luna® CA³, and the associated documentation. The product design documentation, in addition to the guidance documentation, was evaluated from a security perspective.

The evaluation analysis activities involved a structured evaluation of the product documentation in the following areas:

1. Configuration Management (CM automation, CM capabilities, CM scope);
2. Delivery and Operation (delivery, secure installation, generation and start-up);
3. Design Development (functional specification, informal security policy model, high-level and low-level design, implementation representation and requirements traceability);
4. Guidance (administrator and user guidance);
5. Life Cycle Support (development security, life cycle definition, tools and techniques, and flaw remediation);
6. Testing (developer's coverage and depth analysis, functional testing, and independent functional and vulnerability testing); and
7. Vulnerability Assessment (strength of function, misuse, and vulnerability analyses).

An analysis and an examination of the Luna® CA³, the development environment, and the associated CM documentation were performed.

The evaluators examined the delivery documentation and determined that it sufficiently describes all procedures to maintain integrity and the detection of modification or substitution of the TOE when distributing the TOE to the user's site.

The evaluators examined the installation, generation, and start-up procedures and determined that the procedures describe the installation, generation, and start-up of the TOE in sufficient detail to result in a secure configuration.

The evaluators examined the design development documentation and determined that the documentation sufficiently describes the design, interfaces, and functions of the product.

The evaluators examined the development environment and processes used in the development and maintenance of the TOE.

The evaluators examined the guidance documentation and determined that the documentation sufficiently describes how to securely use and administer the product.

The Luna® CA³ security target's claims for the strength of function and the developer's vulnerability, misuse, and SOF analyses were validated through independent evaluator analysis.

The evaluators examined the developer's security controls on the development environment to ensure that they provide confidentiality and integrity of the TOE design and implementation, ensuring that secure operation of the TOE is not compromised.

The evaluators examined the developer's documented model of the TOE life cycle.

The evaluators examined the developer's development tools to ensure that they are well defined and that they yield consistent and predictable results.

The evaluators examined the developer's flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. Additionally, the evaluators examined the developer's procedures to ensure that they provide for the correction of security flaws, for the receipt of flaw reports from TOE users, and for assurance that the corrections introduce no new security flaws.

All activities for the evaluation of the security target and the evaluation of the Luna® CA³ resulted in a PASS verdict. These verdicts resulted from evaluation activities performed at EWA-Canada and several site visits to the Chrysalis-ITS head office in Ottawa, Ontario, Canada.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests. During this evaluation, the evaluators developed independent tests by examining the design and guidance documentation, examining developer vulnerability analysis, and repeating a subset of developer tests.

12.1 Testing Coverage

The developer provided test documentation comprised of a test suite and an analysis of both coverage and depth. The tests focused on the security functional requirements defined in the ST and the security functions defined in the functional specification.

12.2 Penetration Testing

Penetration tests were devised using the Luna® CA³ vulnerability analysis and associated misuse and strength of function analyses, the functional specification, the high-level design, the low-level design, the PKCS#11 standard, the ST, and the Planning and Integration Guide. The tests focused on gaining access to security data, denial of service, and session hijacking.

12.3 Conduct of Testing

All testing took place at EWA-Canada and was subject to oversight by the CCS CB. To perform the testing, the evaluators used public domain tools for development of new testing applications. The evaluators also used developer-supplied test tools and created test procedures to examine the results from the TOE.

12.4 Results

The developer tests and independent functional tests yielded the expected results, giving assurance that the TOE behaves as specified in the ST and the design documentation. The penetration testing received a PASS verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities of the Luna® CA³ in the intended operating environment while assuming the role of an attacker possessing an attack potential of LOW.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 level of assurance, augmented with ALC_FLR.2 *Flaw Remediation*. All evaluation activities resulted in a PASS verdict. These results are supported by evidence contained in the *Evaluation Technical Report*.

14 Evaluator Comments, Observations and Recommendations

The user of TOE should ensure that the security assumptions for the intended environment are followed and that the original installation media be protected in the same manner as the TOE itself. IT Security best practices should be followed and all non-essential software and applications should be uninstalled or disabled on the Luna® CA³ host computer system.

In addition to the TOE software, the developer also offers a Luna® CA³ Developer's Kit, which is a useful tool for writing PKCS#11-compliant applications that can effectively use the Luna® CA³ system.

15 Acronyms and Abbreviations

Acronym/Abbreviation	Description
ANSI	American National Standards Institute
CA	Certificate Authority
CB	Certification Body
CC	Common Criteria for IT Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PKI	Public Key Infrastructure
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation

16 Final Interpretations

The following interpretations have been applied to the CC for this evaluation.

Table 1 - Final Interpretations

Number	Interpretation Title
003	Unique identification of configuration items in the configuration list
004	ACM_SCP.*.1C requirements unclear
013	Multiple SOF claims for multiple domains in a single TOE
016	Objective for ADO_DEL
025	Level of detail required for hardware descriptions
027	Events and actions
031	Obvious vulnerabilities
032	Strength of Function Analysis in ASE_TSS
037	ACM on Product or TOE?
051	Use of 'documentation' without C&P elements
055	Incorrect Component referenced in Part 2 Annexes, FPT_RCV
058	Confusion over refinement
062	Confusion over source of flaw reports
064	Apparent higher standard for explicitly stated requirements
069	Informal Security Policy Model
074	Duplicate informative text for ATE_COV.2-3 and ATE_DPT.1-3
075	Duplicate informative text for different work units
080	Work unit does not use `shall examine to determine'
084	Aspects of objectives in TOE and environment
085	SOF Claims additional to the overall claim
092	Release of the TOE
094	FLR Guidance Documents Missing
095	SCP Dependency in ACM_CAP
116	Indistinguishable work units for ADO_DEL
120	Indistinguishable work units for ADO_DEL
127	Work unit not at the right place
128	Coverage of the delivery procedures
133	Consistency analysis in AVA_MSU.2

17 References and Bibliography

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

1. *Common Criteria for Information Technology Security Evaluation, Version 2.1*;

2. *CCS#4, Technical oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 0.84 - Draft*;

3. *Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation Methodology, Version 1.0*;

4. *Common Methodology for Information Technology Security Evaluation, CEM-99/045, version 1.0, August 1999 Part 2: Evaluation Methodology Incorporated with interpretations as of 2002-02-28;*

5. *Security Target for Luna® CA³ Firmware Version 3.97, Software Releases 8.0 and 8.1, Version 12, dated 1 November 2002*;

6. *Luna® PKI HSM Installation Guide - 800193-000 Rev. A;*

7. *Luna® PKI HSM Planning and Integration Guide – 800194-000 Rev. A;*

8. *FIPS 140-1 Certificate #214 issued under the CMVP (URL: http://csrc.nist.gov/cryptval/140-1/140crt/140crt214.pdf);*

9. *Evaluation Technical Report (ETR), EWA-Canada Document No. 1431-000-D002, Version 1.6, dated 6 November 2002;* and

10. *Common Evaluation Methodology for Information Technology Security Evaluation Supplement ALC_FLR Flaw Remediation, CEM-2001/0015R, Version 1.1, February 2002.*