Certification Report

EAL 4+ Evaluation of Entrust Authority Security Manager and Security Manager Administration v8.1 SP1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-127-CR
Version: 1.0
Date: 06 February 2012
Pagination: i to iii, 1 to 12

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 CGI IT Security Evaluation & Test Facility 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 February 06, 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:

- Entrust Authority is trademark Entrust, Inc.;
- Entrust Entellegence is a trademark of Entrust, Inc.;
- Critical Path Directory Server is a trademark of Entrust, Inc;
- Windows is a registered trademark of Microsoft Corp.;
- PostgreSQL is a trademark of the PostgreSQL foundation.; and
- Luna CA is a trademark of SafeNet, Inc.

TABLE OF CONTENTS

Executive Summary

Entrust Authority Security Manager and Security Manager Administration v8.1 SP1 (hereafter referred to as EA SM & SMA v8.1 SP1), from Entrust, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

EA SM & SMA v8.1 SP1 is a Public Key Infrastructure (PKI) that creates and manages public key certificates. EA SM & SMA v8.1 SP1 supports traditional PKI based on the [X.509] standard, as well as PKI based on the [ISO 7816] standard for a specific application for Extended Access Control (EAC) for electronic passports. EA SM & SMA v8.1 SP1 incorporates FIPS 140-2 validated cryptography.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 19 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 EA SM & SMA v8.1 SP1, 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.

EA SM & SMA v8.1 SP1 is conformant with the *Certificate Issuing and Management Components Protection Profile, Version 1.1, December 27, 2010.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EA SM & SMA v8.1 SP1 evaluation meets all the conditions of the *Arrangement on the 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Entrust Authority Security Manager and Security Manager Administration v8.1 SP1 (hereafter referred to as EA SM & SMA v8.1 SP1), from Entrust Limited.

2 TOE Description

EA SM & SMA v8.1 SP1 is a Public Key Infrastructure (PKI) that creates and manages public key certificates. EA SM & SMA v8.1 SP1 supports traditional PKI based on the [X.509] standard, as well as PKI based on the [ISO 7816] standard for a specific application for Extended Access Control (EAC) for electronic passports. EA SM & SMA v8.1 SP1 incorporates FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for EA SM & SMA v8.1 SP1 is identified in Section 6 of the ST.

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

Cryptographic Module	**Certificate #**
Entrust Base Security Kernel CM version 8.0	*Pending* [2]
Luna CA4 with DOCK-2 USB reader, firmware 4.6.1 and client 2.4 HSM[3] (3rd Party HSM)	1178

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in EA SM & SMA v8.1 SP1:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 186-2 APPENDIX 3	#1253
Advanced Encryption Standard (AES)	FIPS 186-2 APPENDIX 3,	#1923

[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.

[3] Hardware Security Module

Cryptographic Algorithm	Standard	Certificate #
	PUB 197	
Rivest Shamir Adleman (RSA)	FIPS 186-2	#992
Secure Hash Algorithm (SHA-1)	FIPS 180-2	#1689
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	#1158
RSA-PSS	FIPS 186-3	#992
DSA	FIPS 186-2	#610
ECDSA	FIPS 186-3	#275
ECDH	SP800-56A	#15

4 Security Target

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

Title: Entrust Authority Security Manager and Security Manager Administration
Version: 5.5
Date: 17 January 2012

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.*

EA SM & SMA v8.1 SP1 is:

a. *Common Criteria Part 2 extended*, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

- FCO_NRO_CIMC.3: Enforced proof of origin and verification of origin;
- FCO_NRO_CIMC.4: Advanced verification of origin;
- FCS_CKM_CIMC.5: CIMC private and secret key zeroization;
- FCS_SOF_CIMC.1: CIMC Strength of Functions;

- FDP_ACF_CIMC.2: User private key confidentiality protection;
- FDP_ACF_CIMC.3: User secret key confidentiality protection;
- FDP_CIMC_CER.1: Certificate Generation;
- FDP_CIMC_CRL.1: Certificate revocation list validation;
- FDP_CIMC_CSE.1: Certificate status export;
- FDP_ETC_CIMC.5: Extended user private and secret key export;
- FDP_SDI_CIMC.3: Stored public key integrity monitoring and action;
- FMT_MOF_CIMC.3: Extended certificate profile management;
- FMT_MOF_CIMC.5: Extended certificate revocation list profile management;
- FMT_MTD_CIMC.4: TSF private key confidentiality protection;
- FMT_MTD_CIMC.5: TSF secret key confidentiality protection;
- FMT_MTD_CIMC.7: Extended TSF private and secret key export; and
- FPT_CIMC_TSP.1: Audit log signing event.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
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.
d. EA SM & SMA v8.1 SP1 is conformant with the *Certificate Issuing and Management Components Protection Profile, Version 1.1, December 27, 2010.*

6 Security Policy

EA SM & SMA v8.1 SP1 implements the CIMC TOE Access Control Policy, a role-based access control policy to control user access to the system; details of this security policy can be found in Section 6.1 of the ST.

In addition, EA SM & SMA v8.1 SP1 implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EA SM & SMA v8.1 SP1 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:

- Audit logs are required for security-relevant events and must be reviewed by the Auditors;
- An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.);
- Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner;
- All Administrators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated;
- Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility);
- Malicious code destined for the TOE is not signed by a trusted entity;
- Administrators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data;
- General users, Administrators, Officers and Auditors are trained in techniques to thwart social engineering attacks; and
- Competent Administrators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the CIMC PP, as identified in this ST.
- The TOE is physically protected against loss of communications i.e., availability of communications.
- The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

7.3 Clarification of Scope

EA SM & SMA v8.1 SP1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. EA SM & SMA v8.1 SP1 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for EA SM & SMA v8.1 SP1comprises:

- Entrust Authority Security Manager v8.1 SP1 (build number 8.1.350.240); and
- Entrust Authority Security Manager Administration v8.1 SP1 (build number 8.1.350.175).

Additional Software Requirements:

- Database - Postgresql 8.3.7;
- Directory - Critical Path Inc., Directory Server (DS) 5.01; and
- End User Client Systems - Entrust Entelligence Security Provider (ESP) 9.2 on Microsoft Windows 7.

Additional Hardware Requirements:

- HSM - Luna CA4 with DOCK-2 USB reader, firmware 4.6.1 and client 2.4.

The documents required to put the TOE into its evaluated configuration are:

- Entrust Authority Security Manager 8.1 Guidance Documents (AGD_OPE.1) version 1.4 is a high-level document detailing references from existing operational guidance for the secure configuration of the TOE in it’s evaluated configuration and environment;

- Entrust Authority Security Manager Administration 8.1 SP1 Installation Guide Issue 1.0 is the commercially available user guidance that provides a comprehensive reference on setting up and using the TOE;

- Entrust Authority Security Manager Administration 8.1 SP1 Operations Guide Issue 1.0 is the commercially available user guidance that provides a comprehensive reference on operating the TOE; and

- Entrust Authority Security Manager 8.1 Preparative Procedures (AGD_PRE.1) v1.3 provides supplemental information specific to the configuration of the TOE in the Common Criteria Evaluated Configuration.

9 Documentation

The Entrust documents provided to the consumer are as follows:

- Entrust Authority Security Manager 8.1 Guidance Documents (AGD_OPE.1) version 1.4;

- Entrust Authority Security Manager Administration 8.1 SP1 Installation Guide 1.0;

- Entrust Authority Security Manager Administration 8.1 SP1 Operations Guide Issue 1.0; and

- Entrust Authority Security Manager 8.1 SP1 Preparative Procedures (AGD_PRE.1) v1.3.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EA SM & SMA v8.1 SP1, including the following areas:

Development: The evaluators analyzed the EA SM & SMA v8.1 SP1 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the EA SM & SMA v8.1 SP1 security architectural description and determined that the initialization process is 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 EA SM & SMA v8.1 SP1 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 EA SM & SMA v8.1 SP1 configuration management system and associated documentation was performed. The evaluators found that the EA SM & SMA v8.1 SP1 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 unauthorized 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 EA SM & SMA v8.1 SP1 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 EA SM & SMA v8.1 SP1 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 Entrust for EA SM & SMA v8.1 SP1. 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 include if ALC_FLR.2 is claimed.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of EA SM & SMA v8.1 SP1. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the EA SM & SMA v8.1 SP1 in its operational environment.

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[4].

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 CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer tests to gain a deeper understanding of the TOE and the TOE interfaces. All security functions and interfaces were exercised;

b. Security Audit: The objective of this test goal is to determine the TOE's ability to audit the activity of users;

c. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized users only and that password rules are followed;

d. Access Control: The objective of this test is to demonstrate that access rules are in place;

e. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data by verifying for digital signatures;

f. Key Management: The objective of this test goal is to demonstrate the protection of public keys as well as the user export/import function and the user archive/retrieval function;

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

g. Certificate management and revocation: The objective of this test goal is to verify the management of certificate profiles; and

h. Remote Data Entry and Export: The objective of these tests is to demonstrate that data exchanged via PKIX-CMP is protected for confidentiality and integrity.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Port Scan: The purpose of this test case is to identify all open ports on the TOE;

b. Traffic Interception: The purpose of this test is to demonstrates that data exchanged via SEP, PKIX-CMP, or GUI is protected for confidentiality and integrity;

c. Tampering – Log Files: This test demonstrates that modifying log file results in log file no longer being valid;

d. Memory Scanning: The purpose of this test is to demonstrate that passwords cannot be found in memory after use; and

e. Tampering – SQL Injection: The purpose of this test case is to try and bypass the normal authentication mechanism by injecting parameters.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

EA SM & SMA v8.1 SP1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Entrust development site at 1000 Innovation Drive, Kanata, Ottawa. 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 EA SM & SMA v8.1 SP1 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 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CP	Certificate Policy
CPL	Certified Products list
CPS	Certification Practices Statement
CIMC	Certificate Issuing and Management Component
CM	Configuration Management
DSA	Digital Signature Algorithm
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ETR	Evaluation Technical Report
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
PKI	Public Key Infrastructure
PP	Protection Profile
PSS	Probabilistic Signature Scheme
RSA	Rivet Shamir Adleman
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TFS	TOE Security Functions
Triple DES	Triple Data Encryption Algoritm
SHA-1	Secure Hash Algoritm

14 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. Certificate Issuing and Management Components Protection Profile, Version 1.1, December 27, 2010.

e. Entrust Authority Security Manager and Security Manager Administration Version 5.5 January 17, 2012.

f. Entrust Authority Security Manager and Security Manager Administration v8.1 SP1 Evaluation Technical Report, version 1.2, January 19, 2012.

g. [X.509] ITU-T Recommendation X.509 (2005 | ISO/IEC 9594-8: 2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

h. [ISO 7816] ISO/IEC 7816: Identification Cards – Integrated Circuit Cards (Parts 10, 11 & 12).