Certification Report

Evaluation of Certificate Issuing and Management Components Protection Profile

Version 1.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-6-3-CR
Version: 1.1
Date: 9 September 2011
Pagination: i to iii, 1 to 6

DISCLAIMER

The Protection Profile (PP) 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 protection profile listed in this certificate and in conjunction with the complete certification report. 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 Protection Profile 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 of the profile 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 DOMUS ITSL located in Ottawa, Canada.

By awarding a certificate, a certifying body asserts that a protection profile complies with the requirements for protection profile (PP) evaluation specified in the Common Criteria for Information Security Evaluation. A protection profile is an implementation-independent set of security requirements for a category of IT that meets specific consumer needs. The objective of a protection profile evaluation is to ensure that the protection profile is complete, consistent, technically sound and, therefore, suitable for use as the basis of security requirements for the relevant category of IT.

The protection profile associated with this certification report is identified by the following nomenclature:

Title: Certificate Issuing and Management Components Protection Profile
Version: 1.5
Date: 11 August 2011

TABLE OF CONTENTS

Executive Summary

Certificate Issuing and Management Components Protection Profile (hereafter referred to as CIMC PP) is the Protection Profile being evaluated.

The Certificate Issuing and Management Components (CIMC) Protection Profile (PP) defines requirements for components that issue, revoke, and manage public key certificates, such as X.509 public key certificates.

This document was derived from the *Certificate Issuing and Management Components Family of Protection Profiles, Version 1.0, October 31, 2001* (CIMC PP). More specifically, this PP has essentially adopted the security functional requirements for Security Level 3 in that PP, while revising the assurance requirements to conform with Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2, and also to update the content from Common Criteria (CC) version 2.1 to CC version 3.1 Revision 3.

The original CIMC PP was developed through a collaborative effort between the US National Institute of Standards and Technology (NIST) and the US National Security Agency (NSA) with the assistance and input of vendors.

DOMUS ITSL is the CCEF that conducted the evaluation. The evaluation was performed using the Common Criteria for Information Technology Security Evaluation (CC) [b], and the Common Methodology for Information Technology Security Evaluation (CEM) [c], and was completed on 25 August 2011. It was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS), and all evaluation activities were performed by the CCEF, in accordance with the CEM.

CIMC PP was evaluated against the APE class of assurance requirements specified in the CC. The evaluation has determined that the CIMC PP is a well-written, mature document, which clearly defines the intended target of evaluation (TOE), and its intended operating environment. It meets all of the CC requirements specified for protection profile evaluation.

Recommendations are provided in this report for those wishing to use or claim conformance to CIMC PP. Communications Security Establishment Canada, as the CCS Certification Body, declares that CIMC PP 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 Identification of Target of Evaluation

1.1 Protection Profile

The evaluated protection profile, the subject of this certification report, is identified by the following nomenclature:

Title: Certificate Issuing and Management Components Protection Profile
Version: 1.5
Date: 11 August 2011

1.2 Protection Profile Developer

The original CIMC PP was developed through a collaborative effort between the United States National Institute of Standards and Technology (NIST) and the United States National Security Agency (NSA) with the assistance and input of vendors. If was then modified for use in Canada by Entrust Limited, through one of the original contributing authors.

1.3 Evaluation Sponsor

The sponsor of the evaluation was Entrust Limited.

1.4 Evaluator

The Common Criteria Evaluation Facility (CCEF) that conducted the evaluation is DOMUS ITSL, located in Ottawa, Canada.

2 Results of the Evaluation

The CIMC PP was successfully evaluated against the requirements of the Protection Profile Evaluation (APE) class of Common Criteria assurance requirements. This means that the PP is technically sound and suitable for use as a statement of security requirements for components that issue, revoke, and manage public key certificates, such as X.509 public key certificates.

The protection profile was found to be a well-written, mature document that clearly defines the intended target of evaluation (TOE). It is comprehensive in its description of the environment in which the intended TOE would operate and the anticipated threats it would face.

3 Evaluation Activities

The evaluation involved an analysis of the CIMC PP against the requirements of the APE class of Common Criteria assurance requirements. The objective of protection profile evaluation is to determine, by analysis, that the specified security requirements are effective at solving the security problem defined for the environment in terms of threats, policies and assumptions. The approach to analysis is pair-wise, whereby the stated security objectives are verified to be effective against the security problem, and the security requirements verified to satisfy the security objectives. Finally, the security requirements are analyzed to determine that they are mutually supportive and cohesive.

The evaluation of the CIMC PP was an iterative process, whereby observations discovered during evaluation resulted in a revision of the CIMC PP and its subsequent re-evaluation.

The evaluation process began in January 2011, with version 1.2 and culminated with the successful evaluation of version 1.5 in August 2011. For all versions, all evaluation activities were performed by the CCEF, in accordance with the Common Methodology for Information Technology Security Evaluation [c].

4 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.*

CIMC PP 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 PP:
   - 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_CIMC_CER.1 Certificate Generation;
   - FDP_CIMC_CRL.1 Certificate Revocation;
   - FDP_CIMC_CSE.1 Certificate status export;
   - FDP_CIMC_OCSP.1 Basic Response Validation;
   - 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_MOF_CIMC.6 OCSP 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.

5 Using the Protection Profile

Those claiming conformance or otherwise using the protection profile should be aware of the following:

1. The CIMC PP contains a large number of security objectives to be met jointly by the TOE and the environment. This is to ensure its applicability to a broad range of product types and implementations. Users should be aware of this and refine the ST to suit the product, technology, and organizational implementation type.

2. As permitted by the Common Criteria, there are a large number of extended security functional requirements that typically extend existing functional requirements for the specific security solution type. All of these functional requirements are detailed in section 6 of the CIMC PP [d]. When claiming compliance to the CIMC PP, ST authors should note these extended security functional requirements and determine that they make sense for the particular TOE conformance.

6 Results of the Evaluation

The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the Evaluation Technical Report (ETR).

7 Evaluator Comments, Observations and Recommendations

7.1 Explicitly stated security requirements

The CIMC PP uses a number of explicitly stated security functional requirements. The reason for using explicitly stated requirements in lieu and in refinement of the ones provided by the Common Criteria is due to the nature of certificate issuing and management components of a PKI.

7.2 Security Objectives for both the TOE and the environment

When developing security targets against this PP or using this PP as the basis for selecting a product, please note that there are a large number of security objectives to be met jointly by the TOE and the environment. A needs and risk assessment should be performed to determine specific requirements for the TOE in order to ensure a satisfactory level of security functionality for the TOE as opposed to the environment.

8 Claiming conformance to protection profiles

One of the benefits of claiming conformance to an evaluated protection profile is the reuse of protection profile evaluation results for a security target evaluation. The following guidelines and restrictions apply when claiming conformance to a protection profile and reusing the protection profile evaluation results.

- A security target cannot claim conformance to a protection profile if it implements only a subset of the security requirements, either functional or assurance, that are specified in the protection profile. A security target may, however, implement a superset of the security requirements specified in a protection profile and claim conformance to that protection profile. A security target may also claim conformance to multiple protection profiles. Security targets that implement a superset of protection profile security requirements, or that claim conformance to more than one protection profile, must by evaluated to determined that the security requirements remain mutually supportive.

- A protection profile to which conformance is claimed may contain uncompleted security requirement operations. A security target claiming conformance to such a protection profile must complete all operations.

9 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
APE	Protection Profile Evaluation
CC	Common Criteria
CCEF	Common Criteria Evaluation Facility
CCRA	Arrangement of Recognition of Common Criteria Certificates
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CIMC	Certificate Issuing and Management Component
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NSA	National Security Agency
NIST	National Institute of Standards and Technology
PALCAN	Program for the Accreditation of Laboratories - Canada
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

10 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 1.5, 11 August 2011

e. Evaluation Technical Report Certificate Issuing and Management Components Protection Profile, Version 1.0, 25 August 2011