Certification Report

Evaluation of Standard Protection Profile for Enterprise Security Management Access Control

Version 2.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-6-4-CR
Version:	1.0
Date:	19 March 2012
Pagination:	i to iii, 1 to 7

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 EWA-Canada 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:

Standard Protection Profile for Enterprise Security Management Access Control

Version 2.0

22 February 2012

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Standard Protection Profile for Enterprise Security Management Access Control (hereafter referred to as ESM AC PP), from the Enterprise Security Management Community, is the Protection Profile being evaluated.

The Enterprise Security Management Access Control Protection Profile (ESM AC PP), version 2.0, developed by the Enterprise Security Management Community (ESMC), describes the information technology (IT) security requirements for access control products which dictate the usage restrictions imposed upon specific authenticated users, roles, or privileges (such as access to information or a process) within an enterprise IT system. The ESM AC PP is one of six protection profiles in the ESM PP family and is meant to be used for one component in an ESM system and not work in isolation. The ESM AC PP was evaluated against the APE class of assurance requirements specified in the Common Criteria (CC).

EWA-Canada 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]. The evaluation process began in June 2011, with version 1.3, and culminated with the successful evaluation of version 2.0 on 29 February 2012. 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.

The ESM AC PP was evaluated against the APE class of assurance requirements specified in the Common Criteria (CC). The evaluation has determined that the ESM AC 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 the ESM AC PP. Communications Security Establishment Canada, as the CCS Certification Body, declares that ESM AC 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:

Standard Protection Profile for Enterprise Security Management Access Control

Version 2.0

22 February 2012

1.2 Protection Profile Developer

The Enterprise Security Management Community (ESMC) developed the protection profile. The members of the ESMC at the time of the drafting of the protection profile included:

Booz Allen Hamilton;
CA Technologies;
Microsoft Corporation;
IBM Corporation;
EMC Corporation;
Cisco Systems, Inc;
CSC;
Oracle Corporation;
Defense Signals Directorate (Australian Scheme);
EWA-Canada;
US National Information Assurance Partnership (NIAP)/Common Criteria Evaluation and Validation Scheme (CCEVS); and
Common Criteria Consulting LLC.

1.3 Evaluation Sponsor

The sponsor of the evaluation was the Enterprise Security Management Community.

1.4 Evaluator

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

2 Results of the Evaluation

The ESM AC 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 Enterprise Security Management Access Control evaluation.

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 ESM AC 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 ESM AC PP was an iterative process, whereby observations discovered during evaluation resulted in a revision of the ESM AC PP and its subsequent re-evaluation. The evaluation process began in June 2011, with version 1.3 and culminated with the successful evaluation of version 2.0 in February 2012. 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.*

ESM AC 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:

- ESM_DSC.1 – Object Discovery;
- FAU_STG_EXT.1 – External Audit Trail Storage;
- FCS_CKM_EXT.4 – Cryptographic Key Zeroization;
- FCS_RBG_EXT.1 – Cryptographic Operation (Random Bit Generation);
- FPT_FLS_EXT.1 – Failure of Communications; and
- FTA_SSL_EXT.1 – TSF-initiated session locking.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL 1 augmented*, containing all security assurance requirements in the EAL 1 package, as well as the following: ASE_OBJ.2 – Security Objectives, ASE_REQ.2 – Derived Security Requirements, and ASE_SPD.1 – Security Problem Definition.

5 Using the Protection Profile

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

1. The intent of the ESM family of Protection Profiles is to define a discrete set of security services which are required in order to facilitate a consistent organizational security strategy. This PP focuses on access control decision and enforcement. A product[1] that conforms to this Protection Profile consumes a centrally-defined access control policy and enforces it. These policies will determine what objects should be protected in the Operational Environment, what subjects are allowed to access these objects, and what set of operations this access is allowed to encompass.

2. The PP does not prescribe any specific type of access control. Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), or other policies can be deployed if they are capable of enforcing the desired access control mechanism.

3. The ESM AC PP is one of six protection profiles in the ESM PP family and is meant to be used for one component in an ESM system and not work in isolation. Products claiming conformance to this protection profile must identify compatible environmental products that conform to the other protection profiles identified in section 7.1 of this report. If the TOE performs functionality that is compatible with multiple protection profiles, then conformance to all applicable protection profiles must be claimed.

4. The TOE may be deployed as hardware or software, as a redundant distributed system, one of a collection of client endpoints, or as a single agent that resides on a server on network boundary device.

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 Related Protection Profiles

The following Protection Profiles will complement this Protection Profile:

[1] The various products within an ESM system may be distinct products, or they may simply be functional capabilities within a larger product described in the ST.

Standard Protection Profile for ESM Policy Management;

Standard Protection Profile for ESM Identity and Credential Management;

Standard Protection Profile for ESM Audit Management;

Standard Protection Profile for ESM Secure Configuration Management; and

Standard Protection Profile for ESM Authentication Server.

7.2 Explicitly stated security requirements

The ESM AC PP defines a new class, Class ESM: Enterprise Security Management. This PP also contains extended components definition for Class FAU: Security Audit, Class FCS: Cryptographic Support, Class FPT: Protection of the TSF, and Class FTA: TOE Access.

Class FCS: Cryptographic Support should only be claimed in the event of the TOE performing its own internal cryptographic functionality and not relying on an Operating System (OS) or cryptographic library to perform the functionality.

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.

1. A security target cannot claim conformance to a protection profile if it implements a subset of the security requirements, either functional or assurance, 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.

2. A security target which claims conformance to a protection profile, but contains a superset of the security requirements, must clearly identify the additional requirements as well as any additional security objectives, threats, organizational security policies and assumptions.

3. 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
ABAC	Attribute Based Access Control
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
CPL	Certified Products list
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ESM	Enterprise Security Management
ESM AC PP	Enterprise Security Management Access Control Protection Profile
ESMC	Enterprise Security Management Community
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MAC	Mandatory Access Control
NSA	National Security Agency
NIST	National Institute of Standards and Technology
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
PP	Protection Profile
RBAC	Role Based Access Control
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. Standard Protection Profile for Enterprise Security Management Access Control, v2.0, 22 February 2012.

e. Evaluation Technical Report (ETR) for Common Criteria Evaluation of Standard Protection Profile for Enterprise Security Management Access Control, Common Criteria Evaluation Number: 383-6-4, Document No.1710-006-D002, Version 1.2, 29 February 2012.