Communications Security Establishment Centre de la sécurité des télécommunications

UNCLASSIFIED

COMMON CRITERIA CERTIFICATION REPORT

CA Privileged Access Manager Version 2.5.5

v1.2
8 August 2016

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. This certification report, and its associated certificate, applies 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 Canadian CC Scheme, 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, 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, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

CA Privileged Access Manager Version 2.5.5 (hereafter referred to as the Target of Evaluation or TOE), from CA, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE enables enterprises to secure the access to critical infrastructure by enforcing configured policies to limit connectivity between users (including privileged users) and targets. The Privileged Access Manager (PAM) Server acts as the Policy Manager (PM) for the PAM product components, enabling policies to be configured and distributed to access control components.

The PAM Server GUI enables administrators to configure policies controlling what users may access what target devices, and using what access mechanisms (protocols). The policies operate within a "deny all, permit by exception" model. Attributes for users (subjects) and targets (objects) may be defined, and policies specify authorized connections between the configured users and targets. The policies may also specify whether users are permitted to connect to a third system after connecting to a target according to a policy.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 26/04/2016 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance 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.

Communications Security Establishment, as the Certification Body, declares that the TOE 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 (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	CA Privileged Access Manager Version 2.5.5
Developer	CA, Inc.
Conformance Claim	Protection Profile - Enterprise Security Management - Policy Management Version 2.1

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.2 TOE DESCRIPTION

The TOE enables enterprises to secure the access to critical infrastructure by enforcing configured policies to limit connectivity between users (including privileged users) and targets. The Privileged Access Manager (PAM) Server acts as the Policy Manager (PM) for the PAM product components, enabling policies to be configured and distributed to access control components.

The PAM Server GUI enables administrators to configure policies controlling what users may access what target devices, and using what access mechanisms (protocols). The policies operate within a “deny all, permit by exception” model. Attributes for users (subjects) and targets (objects) may be defined, and policies specify authorized connections between the configured users and targets. The policies may also specify whether users are permitted to connect to a third system after connecting to a target according to a policy.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

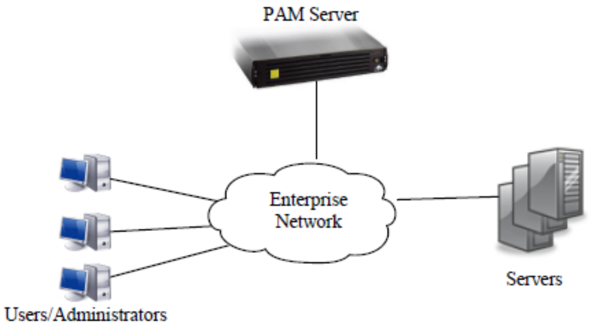

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Audit
- Credential Protection
- Management
- Policy Management
- Secure Communications
- Web Session Management
- Cryptographic Support

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP:

Table 2 Cryptographic Modules

Cryptographic Module	Certificate Number
Luna® PCI-e Cryptographic Module (Hardware Versions: VBD-05-0100, VBD-05-0101 and VBD-05-0103; Firmware Version: 6.2.1)	#1693
OpenSSL FIPS Object Module (Software version: v2.0.9)	#1747

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- The TOE will be able to establish connectivity to other Enterprise Security Management (ESM) products in order to share security data.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The Operational Environment will provide mechanisms to the TOE that reduces the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive validated identity data from the Operational Environment.

3.2 CLARIFICATION OF SCOPE

Although the TOE is an ESM policy management product, it is also a compatible access control product. The access control components on the PAM Server and the Socket Filter Agents (SFAs) are compatible access control products. A complete Access Policy is distributed to the access control components on the PAM Server, while just the Socket Filter portion of an Access Policy is distributed to SFAs. The TOE makes no claim to the Protection Profile for Enterprise Security Management-Access Control Version 2.1.

Cryptographic module #1747 is being claimed as "Vendor Affirmed" in accordance with the CMVP implementation guidance IG.5.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- The TOE software (Privileged Access Manager Version 2.5.5) installed on X304L appliance (PAMHAH995) with the Safenet Luna PCI-E 1700 (VBD-05-0103)

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. CA Privileged Access Manager Hardware Model X304L Setup Guide, Version 4, 1 December 2015

b. CA Privileged Access Manager Reference Guide 2.5, Document Version 2, March 18,2016

c. CA Privileged Access Manager Peripheral Implementation Guide 2.5, Document Version 2, March 18, 2016

d. CA Privileged Access Manager Common Criteria Supplement 2.5, 4 December 2015

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the TOE functional specification and design documentation; 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 TOE security architectural description and determined that the initialization process is secure, 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.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

6 TESTING ACTIVITIES

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

6.1 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.

The evaluators analyzed the developer’s test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance actvities listed in the claimed PP; and

b. Connecting with unsupported cipher suites: The evaluator attempted to connect to the TOE using unsupported cipher suites to confirm that the connection would be denied.

6.3.1 FUNCTIONAL TEST RESULTS

The developer’s tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

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

a. Automated vulnerability scanning: The evaluator used a variety of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities, such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. Information Leakage Verification: The evaluator monitored the TOE for information leakage during start up, shutdown, login, and other scenarios.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
CCS Publication #4, Technical Oversight, Version 1.8, October 2010.
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
CA Privileged Access Manager Security Target, Version 1.13, 20 July 2016
ETR for ESM PM PP CC evaluation of CA, Inc. CA Privileged Access Manager v2.5.5, v1.2, 21 July 2016