Certification Report

CloudMask Engine v2.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-313-CR
Version: 1.0
Date: 27 October 2015
Pagination: i to iii, 1 to 10

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 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 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, 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.

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.

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 CSC Security Testing/Certification Laboratories.

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.

This certification report is associated with the certificate of product evaluation dated 27 October 2015, 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).

TABLE OF CONTENTS

Executive Summary

CloudMask Engine v2.0, from CloudMask Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that CloudMask Engine v2.0 meets the requirements of Evaluation Assurance Level (EAL) 2 for the evaluated security functionality.

CloudMask Engine v2.0 is a software application that enables users to protect their sensitive data while leveraging public and/or private cloud applications. The TOE works transparently by intercepting application data before it is transmitted to the cloud and replaces it with a random token representing the data in a process called tokenization. The tokenized data, referred to as a "mask", is transmitted to the cloud application and is meaningless unless viewed by an authorized CloudMask user. The TOE also invokes the Entrust ESP v9.2 cryptographic engine to encrypt the original data, preventing unencrypted data from leaving the TOE. The CloudMask Manager is a storage repository for the generated mask and associated encrypted data.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 27 October 2015 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 CloudMask Engine v2.0, 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 CCS Certification Body, declares that the CloudMask Engine v2.0 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).

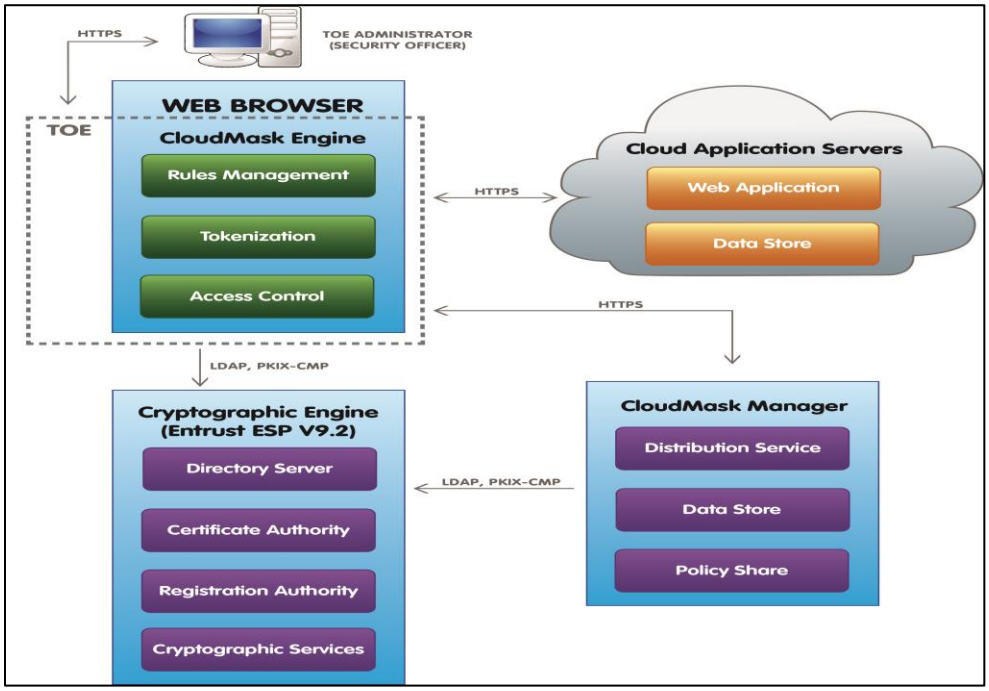
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2 evaluation is CloudMask Engine v2.0, from CloudMask Corporation.

2 TOE Description

CloudMask Engine v2.0 is a software application that enables users to protect their sensitive data while leveraging public and/or private cloud applications. The TOE works transparently by intercepting application data before it is transmitted to the cloud and replaces it with a random token[1] representing the data in a process called tokenization. The tokenized data, referred to as a "mask[2]", is transmitted to the cloud application and is meaningless unless viewed by an authorized CloudMask user. The TOE also invokes the Entrust ESP v9.2 cryptographic engine to encrypt the original data, preventing unencrypted data from leaving the TOE. The CloudMask Manager is a storage repository for the generated mask and associated encrypted data.

A diagram of the CloudMask Engine v2.0 architecture is as follows:



[1] Data generated to replace user data in cloud applications.

[2] Tokenized data.

3 Security Policy

CloudMask Engine v2.0 implements a role-based access control policy to control administrative access to the system. In addition, CloudMask Engine v2.0 implements policies pertaining to the following security functional classes:

- Security Audit
- Identification and Authentication
- User Data Protection
- Security Management
- Protection of the TSF
- Trusted Path/Channels

4 Security Target

The ST associated with this Certification Report is identified below:

CloudMask Engine v2.0 Security Target, Version 2.1, October 22, 2015

5 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.

CloudMask Engine v2.0 is:

a. EAL 2 conformant, with all security assurance requirements listed for EAL 2.
b. Common Criteria Part 2 conformant; with security functional requirements based only upon functional components in Part 2.
c. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of CloudMask Engine v2.0 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- TOE Administrators are trusted and available to perform management functions.

6.2 Clarification of Scope

The Entrust ESP v9.2 cryptographic engine must be implemented in the operational environment to interface with the TOE to generate, distribute, and maintain cryptographic keys and digital certificates, perform cryptographic operations, and provide mechanisms for identifying and authenticating end users.

7 Evaluated Configuration

The evaluated configuration for CloudMask Engine v2.0 comprises the CloudMask Engine software application v2.0 build 610 running on Microsoft Windows 7 with Microsoft Internet Explorer 11 and Microsoft Windows 2008 R2 with Microsoft Internet Explorer 11.

The TOE requires the following components as part of the operational environment:

- CloudMask Manager; and
- Entrust ESP v9.2.

The publication entitled Deployment for Enterprise - Common Criteria, version 2.0.610 describes the procedures necessary to install and operate CloudMask Engine v2.0 in its evaluated configuration.

8 Documentation

The CloudMask Corporation documents provided to the consumer via the CloudMask Enterprise Knowledge Base for version 2.0.610 (https://support.cloudmask.com) are as follows:

a. Management Overview for Enterprise, version 2.0.610;

b. Application Management for Enterprise, version 2.0.610;

c. Deployment for Enterprise, version 2.0.610; and

d. Deployment for Enterprise – Common Criteria, version 2.0.610.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of CloudMask Engine v2.0, including the following areas:

Development: The evaluators analyzed the CloudMask Engine v2.0 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 CloudMask Engine v2.0 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.

Guidance Documents: The evaluators examined the CloudMask Engine v2.0 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 CloudMask Engine v2.0 configuration management system and associated documentation was performed. The evaluators found that the CloudMask Engine v2.0 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 CloudMask Engine v2.0 during distribution to the consumer.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

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

10.1 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[3].

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.

10.2 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. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Audit Events: The objective of this test goal is to confirm that defined audit events are generated and audit records can be reviewed;

c. Trusted Channel: The objective of this test goal is to confirm that HTTPS is used for the transmission of tokenized data for storage; and

d. Default Policies: The objective of this test goal is to confirm that the TOE enforces default element rules[4] and protects the data in accordance with the defined element rules.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Predictable Tokenization: The objective of this test goal is to attempt to derive sensitive user data from collected tokens;

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

[4] Rules that define the data elements to be encrypted and the applicable algorithm used to encrypt/decrypt data.

c. Code Tampering: The objective of this test goal is to attempt to load a modified version of the TOE;

d. Misuse: The objective of this test goal is to attempt to submit data to a protected application while the TOE is disabled; and

e. Encryption Implementation Flaws: The objective of this test goal is to attempt to observe clear text keys or user data.

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

10.4 Conduct of Testing

CloudMask Engine v2.0 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that CloudMask Engine v2.0 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. CloudMask Engine v2.0 Security Target, Version 2.1, October 22, 2015.

e. Evaluation Technical Report, CloudMask Engine v2.0, Document Version 1.0, October 27, 2015.