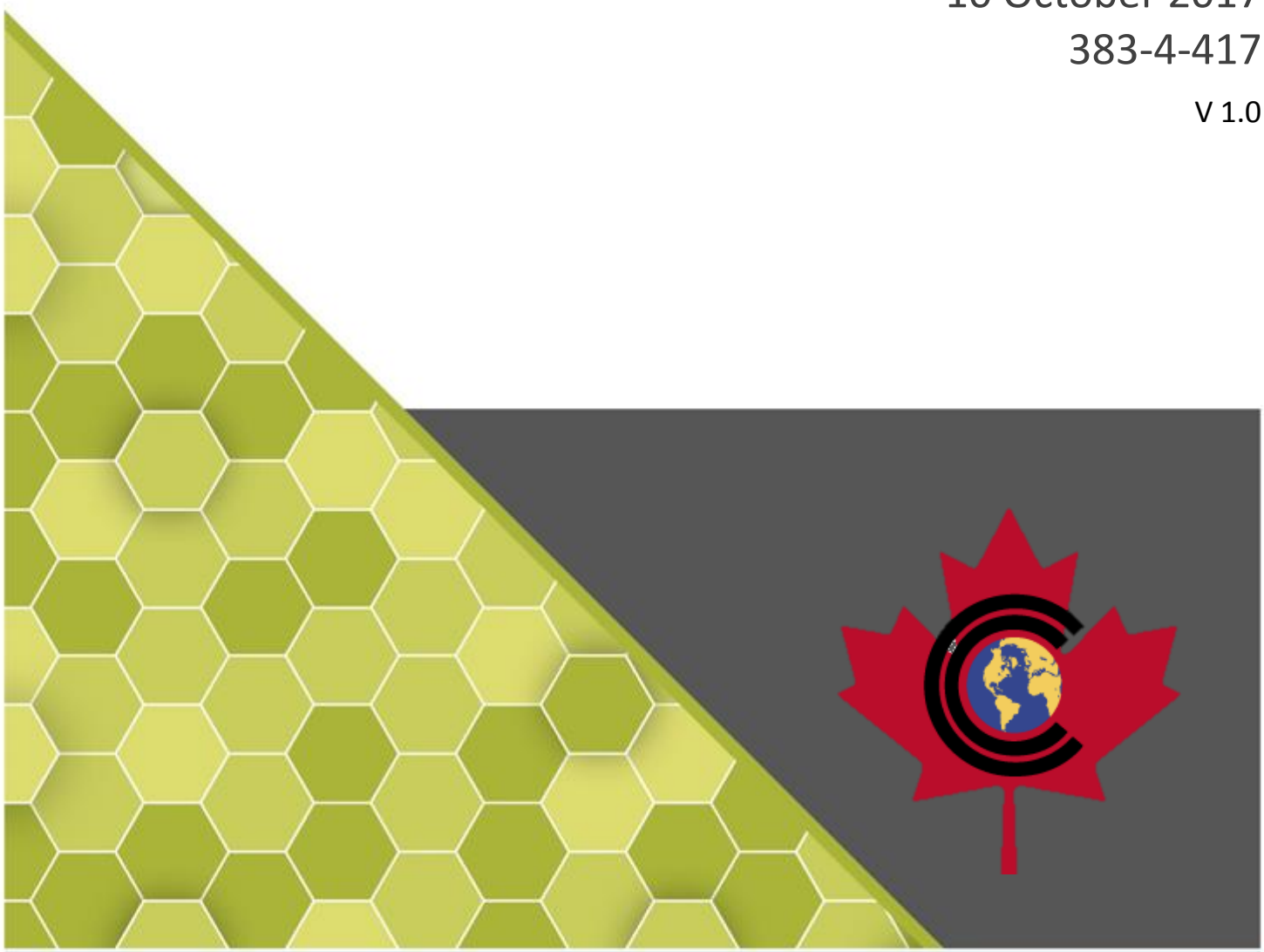
COMMON CRITERIA CERTIFICATION REPORT

CA Technologies CA API Gateway v9.2

10 October 2017

383-4-417

V 1.0



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 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. 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.

By awarding a Common Criteria certificate, the 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 Technologies CA API Gateway v9.2 (hereafter referred to as the Target of Evaluation, or TOE), from CA Technologies, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed 10 October 2017 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 Canadian 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 Technologies CA API Gateway v9.2
Developer	CA Technologies
Conformance Claim	Exact conformance to: • Standard Protection Profile for Enterprise Security Management Policy Management, v2.1, 24 October 2013 (ESM Policy Manager PP); and • Standard Protection Profile for Enterprise Security Management Access Control, v2.1, 24 October 2013 (ESM Access Control PP) – Architectural Variation: Web Based Access Control.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

1.2 TOE DESCRIPTION

The TOE is an enterprise API Management and security solution that provides centralized API management and access control over SOAP web service APIs. The TOE controls how APIs are exposed to and accessed by external client applications.

The TOE is comprised of two main components:

- **Policy Manager.** A GUI application that provides the user with the primary administrative interface to the Gateway. The Policy Manager is used to construct policies and administer the TOE; and

- **Gateway.** One or more hardware or virtual appliances that enforce policy assertions to control web services. Basic configuration is performed using the Gateway Configuration Utility – a menu based Command Line Interface (CLI). The Gateway consumes policies defined by the Policy Manager which also provides the primary administrative interface.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

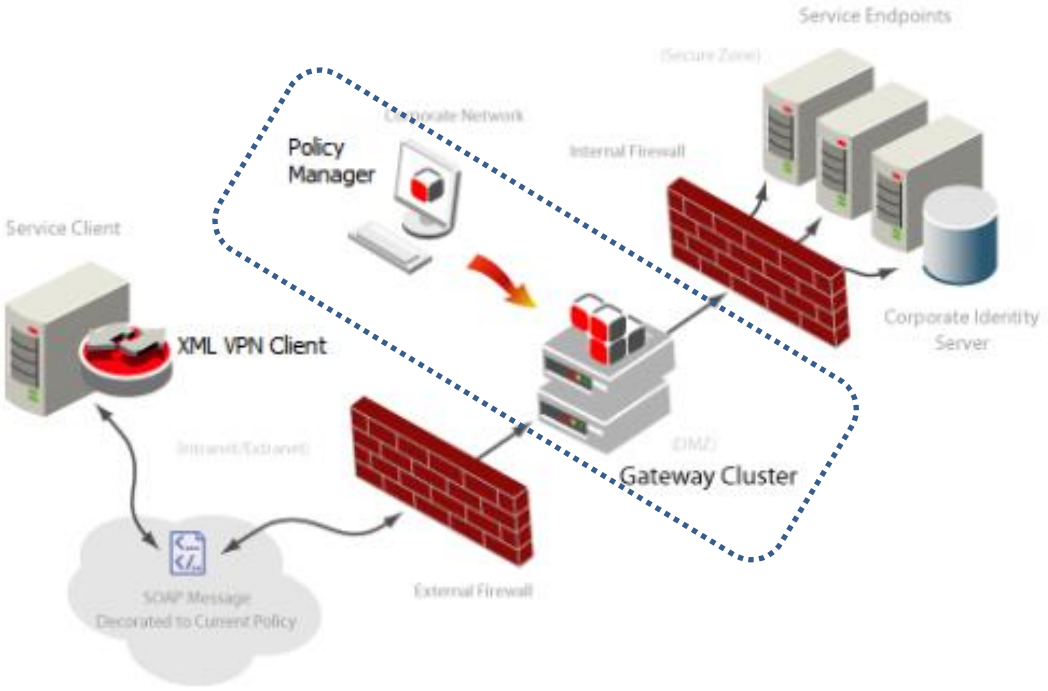


Figure 1 TOE Architecture

2 SECURITY POLICY

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

- Security Audit;
- Communication;
- Cryptographic Support;
- User Data Protection;
- Identification and Authentication;
- Security Management;
- Protection of the TSF;
- Resource Utilization;
- TOE Access; and
- Trusted Path/Channels.

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP and used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
CryptoComply CCJ 1.0	2483
Thales nShield HSM	2638

The following Government of Canada approved cryptographic algorithms were evaluated by the CAVP and used by the TOE:

Table 3 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Advanced Encryption Standard (AES)	FIPS 197	4429
Rivest Shamir Adleman (RSA)	FIPS 186-4	2570
Secure Hash Algorithm (SHS)	FIPS 180-3	3647
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	2941
Deterministic Random Bit Generation (DRBG)	SP 800-90A	1606

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 ESM products in order to share security data;
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication;
- The TOE will receive a reliable time data from the Operational Environment;
- The TOE will receive identity data from the Operational Environment;
- There will be one or more competent individuals assigned to install, configure, and operate the TOE; and
- The TOE will receive policy data from the Operational Environment.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE, CA Technologies CA API Gateway v9.2 Build: 6904, Patch CA_API_nShieldUpdate_64bit_v12.30.00.L7P comprises the following components:

Policy Manager v9.2 Build 6904. The application software running on non-TOE operating system (Windows 7); and

Gateway v9.2 Build 6904. The CA API Gateway in one of the following form factors:

- **CA API Gateway Appliance .** Gateway ships on hardware appliances configured to use the Thales nShield HSM; and
- **CA API Gateway Soft Appliance.** Gateway ships as a virtual appliance using VMWare vSphere v5.5.0.

4.1 DOCUMENTATION

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

a. CA Technologies CA API Gateway v9.2 Online Documentation (available at https://docops.ca.com/ca-api-gateway/9-2/en); and

b. CA Technologies CA API Gateway v9.2 Secure Installation Guide.

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 documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

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 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 activities listed in the claimed PP.

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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. Fuzz Testing: The evaluator conducted fuzz testing using unexpected inputs and malformed packets on the TOE interfaces.

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 this 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 Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. 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 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.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CC	Common Criteria
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CPL	Certified Products List
CSE	Communications Security Establishment
ESM	Enterprise Security Management
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.

Reference
CA Technologies CA API Gateway v9.2 Security Target, version 1.1, 21 September 2017
Evaluation Technical Report for CA Technologies CA API Gateway v9.2 Security Target, version 1.3, 10 October 2017
Assurance Activity Report for CA Technologies, CA API Gateway v9.2, (ESM Policy Management Protection Profile) Version 1.4, 10 October 2017
Assurance Activity Report for CA Technologies, CA API Gateway v9.2 , (ESM Access Control Protection Profile) Version 1.4, 10 October 2017