Certification Report

API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-267-CR
Version: 1.0
Date: 2 July 2014
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 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.

This certification report is associated with the certificate of product evaluation dated 2 July 2014, 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

API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1 (hereafter referred to as API ION SA5600), from API Technologies, is the Target of Evaluation. The results of this evaluation demonstrate that API ION SA5600 meets the requirements of Evaluation Assurance Level (EAL) 1 for the evaluated security functionality.

API ION SA5600 provides secure administrative access to a variety of devices, using variety a of connection types (e.g., IP, dial-up). The API ION SA5600 provides a scalable, compatible platform for remote services delivery.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 13 June 2014 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 API ION SA5600, 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 API ION SA5600 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).

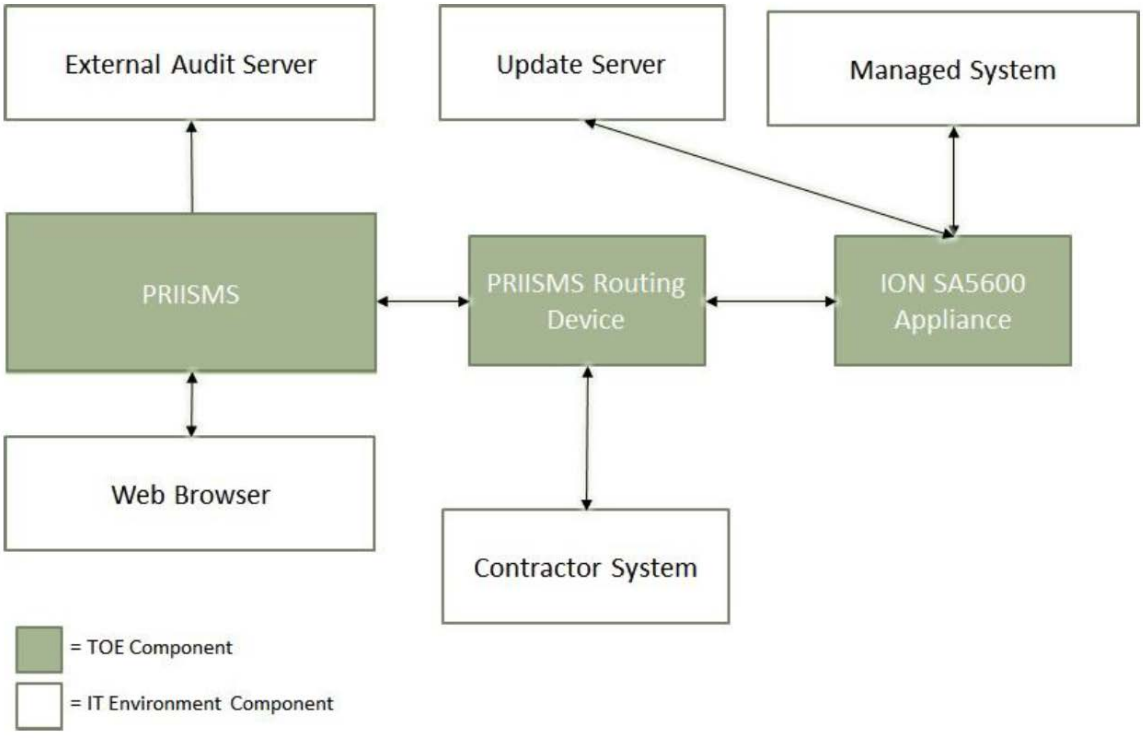
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 1 evaluation is API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1 (hereafter referred to as API ION SA5600), from API Technologies.

2 TOE Description

API ION SA5600 provides secure administrative access to a variety of devices, using variety of connection types (e.g., IP, dial-up). The API ION SA5600 provides a scalable, compatible platform for remote services delivery.

A diagram of the API ION SA5600 architecture is as follows:



3 Security Policy

API ION SA5600 implements a role-based access control policy to control administrative access to the system. In addition, API ION SA5600 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TSF*
- *TOE Access*
- *Trusted Path/Channel*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
Common Crypto Module for PRIISMS, PRIISMS RD, SA5600-IA and NetGard MFD (Software Version: 1.0)	*#2070*
Microsoft Windows Server 2008 R2 Kernel Mode Cryptographic Primitives Library (cng.sys) (Software Versions: 6.1.7600.16385, 6.1.7600.16915, 6.1.7600.21092, 6.1.7601.17514, 6.1.7601.17919, 6.1.7601.17725, 6.1.7601.21861 and 6.1.7601.22076)	*#1335*

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target: API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1, v1.17, 22 May 2014

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.*

API ION SA5600 is:

a. EAL 1 conformant, with all security assurance requirements listed for EAL 1.

b. *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 ST:*

- FAU_STG_EXT.1 - External audit trail storage
- FCS_CKM_EXT.4 - Cryptographic key zeroization
- FCS_RBG_EXT.1 - Cryptographic operation: random bit generation
- FCS_HTTPS_EXT.1 - HTTPS
- FCS_TLS_EXT.1 - TLS
- FIA_PMG_EXT.1 - Password management
- FIA_UIA_EXT.1 - User identification and authentication
- FIA_UAU_EXT.2 - Password-based authentication mechanism
- FPT_SKP_EXT.1 - Protection of TSF data
- FPT_APW_EXT.1 - Protection of administrator passwords
- FPT_TUD_EXT.1 - Trusted update
- FPT_TST_EXT.1 - TSF testing
- FTA_SSL_EXT.1 - TSF-initiated session locking

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 API ION SA5600 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 Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

6.3 Clarification of Scope

The functionality included within the evaluation is limited to the secure management functions listed in the ST, and did not include the primary functionality of the product.

7 Evaluated Configuration

The evaluated configuration for API ION SA5600 comprises:

- *ION SA5600 appliance (SA5610-IA, SA5620-IA, SA5630-IA) running SA5600 firmware v1.3.1 Build 1.3.1-B22;*
- *PRIISMS appliance (PR-5CS-V-IA2, PR-10CS-V-IA2, PR-15CS-V-IA2, PR-25CS-V-IA2, PR-50CS-V-IA2, PR-100CS-V-IA2, PR-200CS-V-IA2) running PRIISMS software v2.8.1 Build 2.8.1; and*
- *PRIISMS Routing Device running PRIISMS Routing Device firmware v1.3.1 Build 1.3.1-B22*

The publication entitled API Technologies Corp. ION PRIISMS & ION SA5600 Secure Appliance Deployment Guide, 22, 28 October 2013 describes the procedures necessary to install and operate API ION SA5600 in its evaluated configuration.

8 Documentation

The API Technologies documents provided to the consumer are as follows:

a. API Technologies Corp. ION PRIISMS & ION SA5600 Secure Appliance Deployment Guide, 22, 28 October 2013*;*

b. ION PRIISMS Administrator Guide, 2.8.1, 21 June 2013;

c. ION Security Appliance 1.3.1 Administrator Guide, 21 March 2013; and

d. API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1 Configuration Items List,1.3, 22 May 2014

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of API ION SA5600, including the following areas:

Development: The evaluators analyzed the API ION SA5600 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the API ION SA5600 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the API ION SA5600 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 API ION SA5600 configuration management system and associated documentation was performed. The evaluators found that the API ION SA5600 configuration items were clearly marked.

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

10 ITS Product Testing

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

10.1 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. Secure Comms: The goal of this test is to confirm the cipher suites that can be used, and will also verify that a weak cipher suite cannot be used;

b. Authentication: The goal of this test is to verify that password entry is secured, password rules are enforced, and that functions are limited by role;

c. Audit Generation: The goal of this test is to verify that the TOE generates audit records for all management functions;

d. Trusted Update: The goal of this test is to confirm that the TOE can be updated with a legitimate update, and that it will reject a false one; and

e. Self test: The goal of this test is to confirm that the TOE can perform a file integrity check on system files.

10.2 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.

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

10.3 Conduct of Testing

API ION SA5600 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.4 Testing Results

The independent functional tests yielded the expected results, providing assurance that API ION SA5600 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for an EAL 1 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. Security Target: API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1, v1.17, 22 May 2014

e. Evaluation Technical Report for EAL 1 Common Criteria Evaluation of API Technologies corp. API Technologies ION SA5600 v1.3.1 with PRIISMS v2.8.1 Document No. 1821-000-D002 Version 1.3, 13 June 2014.