Certification Report

EAL 4+ Evaluation of Intel® SOA Expressway v2.7.0.4 and Intel® SOA Expressway v2.7.0.4 for Healthcare

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Documrnt number:	383-4-121-CR
Version:	1.0
Date:	30 September 2011
Pagination:	i to iii, 1 to 9

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 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 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 Canada, 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 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, 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, Ontario.

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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 30 September 2011, 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).

This certification report makes reference to the following trademarked or registered trademarks:

- Intel is a registered trademark of Intel Corporation in the United States and other countries;
- Linux is a registered trademark of Linus Torvalds; and
- Red Hat is a registered trademark of Red Hat, Inc.

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

TABLE OF CONTENTS

Executive Summary

The Intel® SOA Expressway v2.7.0.4 and Intel® SOA Expressway v2.7.0.4 for Healthcare (hereafter referred to as the SOAE), from Intel, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

The SOAE is a security gateway designed to secure the enterprise Service-Oriented Architecture (SOA). The SOAE provides trust enablement and threat prevention by providing a secure gateway between external service providers and internal services. The SOAE links web services clients to web services servers and web integration servers using administrator defined security rulesets.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 31 August 2011 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 the SOAE , the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 Augmented assurance requirements for the evaluated security functionality. 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*. The following augmentation is claimed:

- ALC_FLR.1 - Basic Flaw Remediation

SOAE is conformant with the *Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.1, July 25, 2007.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the SOAE v2.7.0.4 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and may not be releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Intel® SOA Expressway v2.7.0.4 and Intel® SOA Expressway v2.7.0.4 for Healthcare (hereafter referred to as SOAE), from Intel.

2 TOE Description

The SOAE is a security gateway designed to secure the enterprise Service-Oriented Architecture (SOA). The SOAE provides trust enablement and threat prevention by providing a secure gateway between external service providers and internal services. The SOAE links web services clients to web services servers and web integration servers using administrator defined security rulesets.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the SOAE is identified in Section 6 of the Security Target (ST).

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

Cryptographic Module	Certificate #
Red Hat Enterprise Linux 5 OpenSSH-Server	1384
Red Hat Enterprise Linux 5 OpenSSH Client	1385
Nitrol XL 1600-NFBE HSM Family	1369

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in SOAE:

Cryptographic Algorithm	Standard	Certificate #
Advanced Encryption Standard (AES)	FIPS 197	1160,1161,1162,1265,1266

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Intel® SOA Expressway v2.7.0.4 and Intel® SOA Expressway
v2.7.0.4
for Healthcare Security Target
Version: 1.9
Date: August 30 2011

5 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.*

The SOAE is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based on functional components in Part 2;

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

c. *Common Criteria EAL 4 Augmented, containing all the security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1-Basic Flaw Remediation;* and

d. SOAE is *conformant with the Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.1, July 25, 2007*.

6 Security Policies

SOAE implements three security policies. The Operation Management policy controls user access to the Operation Management process. The Unauthenticated Web Services policy provides a mechanism to configure rulesets to classify unauthenticated incoming HTTP messages. The Authenticated Web Services policy provides a mechanism to configure rulesets to classify authenticated incoming HTTP messages. Details of these security policies can be found in Section 1.5.5 of the ST.

In addition, the SOAE implements policies pertaining to Security Audit, Cryptographic Operation, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilisation and TOE Access. Further details on these security policies may be found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the SOAE product 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

a. Only authorized administrators may access the TOE remotely from the internal and external networks;

b. There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;

c. Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error;

d. The TOE does not host public data; and

e. Information cannot flow among the internal and external networks unless it passes through the TOE.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

a. The TOE is installed and operated in a secure physical environment.

7.3 Clarification of Scope

The SOAE is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration of the SOAE comprises the Intel SOA Expressway v2.7.0.4 Build On 2011-07-15 18:02 running on Red Hat Enterprise Linux 5.4 and browsers Internet Explorer and Firefox.

The publication entitled *Intel® SOA Expressway Installation Guide for Linux OS For Intel® SOA Expressway v2.7, February 2011* describes the procedures necessary to install and operate SOAE in its evaluated configuration.

9 Documentation

The Intel documents provided to the consumer are as follows:

a. Intel® SOA Expressway Installation Guide for Linux OS For Intel® SOA Expressway v2.7, February 2011;

b. Setting up the 2.7 Intel® SOA Expressway Hardware Appliance with FIPS Option, March 2011;

c. Intel® SOA Expressway Management Console User's Guide for Linux OS For Intel® SOA Expressway v2.7, April 2011;

d. Intel® SOA Expressway CLI Guide for Linux OS for Intel® SOA Expressway v2.7, March 2011; and

e. Intel® SOA Expressway Security Reference Guide For Intel® SOA Expressway v2.7, April 2011.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the SOAE, including the following areas:

Development: The evaluators analyzed the SOAE functional specification, design documentation, and a subset of the implementation representation; 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 SOAE security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that the 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 SOAE 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 SOAE configuration management system and associated documentation was performed. The evaluators found that the SOAE configuration items were clearly marked and could be modified and controlled by automated tools. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

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

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the SOAE design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Intel for SOAE. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of SOAE. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the SOAE in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met its testing responsibilities by examining the test evidence, and reviewing the test results, as documented in the ETR[2].

The evaluators analyzed the developer’s test coverage and depth analyses and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer’s tests.

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 was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer’s Installation and Administrative guidance;

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

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator’s TOE installation;

c. Protection of TOE logs: The objective of this test case is to verify the TOE protects the log files by not providing any mechanisms for modifying or deleting the records and relies upon the OS file system access control mechanism;

d. Role-Based access control: The objective of this test case is to verify the Web GUI presents only the commands to the user that the user has access to based on the roles assigned to the user;

e. Authentication system information: The objective of this test case is to verify other than providing an asterisk character when the user enters the password, the Web GUI interface provides only success or failure feedback while the authentication is in progress;

f. Time-out session: The objective of this test case is to verify the session time out mechanism on Web GUI; and

g. Audit sort: The objective of this test case is to verify that thesort function works in the Audit feature.

11.3 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:

- Port scan: The objective of this test case is to identify any suspiciou open ports on the TOE system.

- Bypass: The objective of this test case is to verify that the TOE destroys a session successfully.

- Concurrent Sessions: The objective of this test case is to verify that the TOE manages concurrent sessions successfully;

- Information Leak: The objective of this test case is to verify if any sensitive information leaks in the TOE system;

- Tamper: The objective of this test case is to verify that the TOE is resistent to standard SQL injection attack agains its logon functionality; and

- Communication Failure: The objective of this test case is to verify that the TOE continues to operate when a communications failure has occurred and been resolved.

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

11.4 Conduct of Testing

SOAE 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 Testing (ITSET) Facility at EWA-Canada. 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the SOAE behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is PASS. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The documentation for the SOAE includes a comprehensive Installation and Security Guide.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
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
SOA	Service-Oriented Architecture
ST	Security Target
SQL	Structured Query Language
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 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. Intel® SOA Expressway v2.7.0.4 and Intel® SOA Expressway v2.7.0.4 for Healthcare Security Target, v 1.9, 30 August 2011.

e. Evaluation Technical Report (ETR) SOA Expressway, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-121, Document No. 1627-000-D002, Version 1.4, 31 August, 2011.