Certification Report

EAL 3+ Evaluation of Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-190-CR
Version: 1.0
Date: 13 December 2012
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, 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 CGI Security Evaluation and Test Facility.

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 10 December 2012, 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 registered trademark:

- Solera DeepSee is a registered trademark of Solera Networks Inc.;

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **2**

2 TOE Description **2**

3 Evaluated Security Functionality **2**

4 Security Target **2**

5 Common Criteria Conformance **3**

6 Security Policy **3**

7 Assumptions and Clarification of Scope **3**

7.1 SECURE USAGE ASSUMPTIONS 3
7.2 ENVIRONMENTAL ASSUMPTIONS 4
7.3 CLARIFICATION OF SCOPE 4

8 Evaluated Configuration **4**

9 Documentation **4**

10 Evaluation Analysis Activities **5**

11 ITS Product Testing **6**

11.1 ASSESSMENT OF DEVELOPER TESTS 6
11.2 INDEPENDENT FUNCTIONAL TESTING 6
11.3 INDEPENDENT PENETRATION TESTING 7
11.4 CONDUCT OF TESTING 7
11.5 TESTING RESULTS 8

12 Results of the Evaluation **8**

13 Evaluator Comments, Observations and Recommendations **8**

14 Acronyms, Abbreviations and Initializations **8**

15 References **9**

Executive Summary

Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 (hereafter referred to as Solera DeepSee), from Solera Networks, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Solera DeepSee creates a complete record of network traffic, including both packet headers and payloads. Data crossing the network is captured, indexed, enriched, and saved for future analysis. Once stored, data can be analyzed through the DeepSee interface or shared with other applications to provide additional context and enhanced visibility into network security events.

CGI Security Evaluation and Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 12 October 2012 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 Solera DeepSee, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 3 *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.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Solera DeepSee 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 is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 (hereafter referred to as Solera DeepSee), from Solera Networks.

2 TOE Description

Solera DeepSee creates a complete record of network traffic, including both packet headers and payloads. Data crossing the network is captured, indexed, enriched, and saved for future analysis. Once stored, data can be analyzed through the DeepSee interface or shared with other applications to provide additional context and enhanced visibility into network security events.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Solera DeepSee is identified in Section 6 of the ST.

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

Cryptographic Algorithm	**Standard**	**Certificate #**
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1873
Advanced Encryption Standard (AES) – Electronic Codebook (ECB), Cypher-Block Chaining (CBC)	FIPS 197	2153
Rivest Shamir Adleman (RSA)	FIPS 186-2	1108
Hash Message Authentication Code (HMAC) Secure Hash Algorithm SHA-1	FIPS 198	1318

4 Security Target

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

Title: Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 Security Target
Version: 1.7
Date: 28 September 2012

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*.

Solera DeepSee is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

Solera DeepSee implements a role-based access control policy to control user access to the TOE; details of this security policy can be found in Section 6 of the ST.

In addition, Solera DeepSee implements policies pertaining to security audit, cryptographic support, user data protection, identification and authentication, protection of the TSF, TOE access and trusted path/channels and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Solera DeepSee 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:

- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains;
- The authorized administrators are trusted to follow and apply all administrative guidance in a trusted manner; and
- The TOE software will be protected from unauthorized modification.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is assumed to be deployed in a TOE environment such that the network is configured properly and its size is appropriate for the TOE functionality;
- The TOE is located within a controlled access facility; and
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

7.3 Clarification of Scope

Solera DeepSee offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Solera DeepSee is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Solera DeepSee comprises of the following software:

- Solera DeepSee Software v6.5.0 build 24397; and
- Solera DeepSee Central Manager v6.5.0 build 24397

The TOE can be deployed in a virtual environment as a VMware virtual image or on Solera provided Dell hardware. The software maintains the same functionality whether deployed on the Dell hardware or on an ESX(i) server. Both configurations were evaluated.

The publication entitled Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 Guidance Documentation Supplement, v0.7, describes the procedures necessary to install and operate Solera DeepSee in its evaluated configuration.

9 Documentation

The Solera Networks documents provided to the consumer are as follows:

a. Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 Guidance Documentation Supplement, v0.7;

b. Solera Networks DeepSee Administration Guide, 5 July 2012;

c. Solera Networks DeepSee central Manager Console Guide, 3 July 2012;

d. Solera Networks Installation guide for Dell PowerEdge R720xd Rack Servers, 27 June 2012;

e. Solera Networks DeepSee reference Guide, 5 July 2012; and

f. Solera Networks Installation Guide for VMware ESX Server and Workstation, 6 July 2012.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the Solera DeepSee 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 Solera DeepSee security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Solera DeepSee 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 Solera DeepSee configuration management system and associated documentation was performed. The evaluators found that the Solera DeepSee configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Solera DeepSee design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

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

The evaluators reviewed the flaw remediation procedures used by Solera Networks for Solera DeepSee. During a site visit, the evaluators 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 Solera DeepSee. 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 Solera DeepSee in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 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 their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design 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 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 is the following list of CGI Security Evaluation and Test Facility test goals:

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

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

b. Independent Evaluator testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing: Tests covered in this area include:

- Audit Data generation: The objective of this test goal is to demonstrate proper audit data are generated for login events and that authorized users can view/clear logs.
- User data Protection: The objective of this test goal is to demonstrate the enforcement of Solera access control SFP on captured network traffic data.
- Access Control: The objective of this test goal is to demonstrate only a user with Administrator role can manage TSF data.
- Advisory Message: The objective of this test goal is to validate a default or advisory message regarding unauthorized use of device is displayed before establishing a user session.
- Encryption: The objective of this test goal is to validate that the communications between the Management PC and TOE are encrypted.

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:

a. Disclosure of ports: The objective of this test goal is to scan for open ports to find potential vulnerabilities and services offered by the TOE.

b. Inactivity: The objective of this test goal is to determine if TOE consistently disconnects users due to inactivity.

c. Execute malicious code: The objective of this test case is to attempt to execute malicious code captured in a malicious URL by the TOE.

d. Exhaust DS File System: The objective of this test goal is to generate enormous amount of network traffic to attempt to exhaust the DS file system storage.

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

11.4 Conduct of Testing

Solera DeepSee 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 (ITSET) Facility at CGI 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.

11.5 Testing Results

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

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ 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 evaluator recommends that administrators of the TOE regularly review the Solera Networks Support Center https://support.soleranetworks.com for product's defect and support information.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CBC	Cypher-Block Chaining
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CR	Certification Report
ECB	Electronic Codebook
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
Gbps	Gigabits per second
HMAC	Hash Message Authentication Code
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada

Acronym/Abbreviation/ Initialization	Description
RSA	Rivest Shamir Adleman
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
URL	Uniform Resource Locator

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. Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 Security Target, v1.7, 28 September 2012

e. Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v 6.5.0 ETR, v1.1, 12 October 2012.