Certification Report

EAL 2+ Evaluation of RSA Adaptive Authentication System v6.0.2.1 SP3

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-166-CR
Version: 1.0
Date: 13 April 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 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R3*. 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 13 April 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 trademark:

- RSA®, which is a registered trademark of RSA, The Security Division of EMC.

TABLE OF CONTENTS

Executive Summary

The RSA Adaptive Authentication v6.0.2.1 SP3 (hereafter referred to as RSA Adaptive Authentication), from RSA, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

RSA Adaptive Authentication is a risk-based authentication platform that provides additional layers of security to companies with an online presence. RSA Adaptive Authentication uses positive device identification and risk analysis to ensure that only genuine online customers can access their accounts. RSA Adaptive Authentication provides additional authentication measures during login and continuous monitoring of each transaction. If a single transaction (or series of transactions) exceeds the perceived risk level, the online customer may be challenged to provide additional authentication, or the transaction can be flagged for later review.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 15 March 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 RSA Adaptive Authentication, 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 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 3.1R3*. The following augmentation is claimed:

ALC_FLR.2 – Flaw Reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the RSA Adaptive Authentication System 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) 2 augmented evaluation is RSA Adaptive Authentication System v6.0.2.1 SP3 (hereafter referred to as RSA Adaptive Authentication), from RSA, The Security Division of EMC.

2 TOE Description

RSA Adaptive Authentication is a risk-based authentication platform that provides additional layers of security to companies with an online presence. RSA Adaptive Authentication uses positive device identification and risk analysis to ensure that only genuine online customers can access their accounts. RSA Adaptive Authentication provides additional authentication measures during login and continuous monitoring of each transaction. If a single transaction (or series of transactions) exceeds the perceived risk level, the online customer may be challenged to provide additional authentication, or the transaction can be flagged for later review.

The TOE includes a robust set of administrative applications that make up its Back Office Tools set. These tools are used by TOE administrators for configuring and managing cases, reports, and transaction policies. The Access Management tool provides a single interface for access to the other tools in the suite, and allows administrators to create and manage users and user permissions for these applications.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for RSA Adaptive Authentication is identified in Sections 5 & 6 of the Security Target (ST).

Cryptographic functionality for RSA Adaptive Authentication is provided by a FIPS 140-2-validated cryptographic module: RSA BSAFE Crypto-J JCE Provider Module v4.0, certificate # 1048.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in RSA Adaptive Authentication.

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (Data Encryption Standard)	FIPS 46-3	614
Advanced Encryption Standard (AES)	FIPS 197	669
Secure Hash Algorithm (SHA)	FIPS 180-3	702
Hash based Message Authentication Code (HMAC)	FIPS 198	353
Pseudo Random Number Generator (PRNG)	FIPS 186-2	389
Digital Signature Algorithm (DSA)	FIPS 186-2	251

Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-2	72
Rivest, Shamir, and Adleman (RSA)	ANSI X9.31	311

4 Security Target

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

Title: RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Security Target
Version: 0.5
Date: 31 March 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R3*.

The RSA Adaptive Authentication is:

- Common Criteria Part 2 extended, with security functional requirements based on functional components in Part 2, except for the following explicitly stated requirements defined in the ST;
  - EXT_FCR_ARP.1 – Security Alarms;
  - EXT_FCR_GEN.1 – Case data generation;
  - EXT_FCR_CDA.1 – Potential violation analysis; and
  - EXT_FCR_CDA.2 – Simple attack heuristics.
- Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3; and
- Common Criteria EAL 2 augmented, with all the security assurance requirements in the EAL 2, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

RSA Adaptive Authentication implements a role-based access control policy to control access to Back Office administrative functions of the TOE, an end user access control policy for authenticating to a front-end application employing the TOE and an information flow control policy on end users attempting to perform policy-controlled transactions. Details of these security policies are found in section 6.2 of the ST.

In addition, RSA Adaptive Authentication implements policies pertaining to user data protection, identification and authentication, protection of the TOE security functions (TSF), security management, and case recording and review. Further details on these security polices may be found in section 6.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of RSA Adaptive Authentication 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 Assumption is listed in the ST:

- Personnel authorized to install, configure, and operate RSA Adaptive Authentication are non-hostile, possess appropriate training, will adhere to the procedures for secure usage of the product, and are competent to manage the TOE and the security of the information it contains.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The host machine upon which RSA Adaptive Authentication is installed resides in a controlled access facility.
- The host machine upon which RSA Adaptive Authentication is installed is capable of supporting all of its required functionality.
- The IT environment provides a private network which allows the TOE to provide its security functions to TOE components, the database server, front-end applications, and the RSA Data Center.

7.3 Clarification of Scope

RSA Adaptive Authentication provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks to violate system security. The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communications security.

RSA Adaptive Authentication provides its services and functionality from the various components which are included in the evaluated configuration. One component not included is the eFraudNetwork™ and its connector EFN Agent, which is disabled in the CC-evaluated configuration.

8 Evaluated Configuration.

The evaluated configuration is RSA Adaptive Authentication v6.0.2.1 with Service Pack 3, a software TOE that requires an application server and underlying operating system to run. RSA Adaptive Authentication also relies on the presence of a database application to store data and configurations. For this evaluation, RSA Adaptive Authentication was tested across an array of host operating systems, application web servers, and back-end databases. The matrices are composed from the following:

- Application Web Server: IBM Websphere 7.0, Apache Tomcat 6.0, Red Hat JBoss 5.1.
- Server Operating System: Oracle Solaris 10, Microsoft Windows Server 2003, 2003 R3, 2008, and 2008 R2.
- Database: Oracle 10g, IBM DB2 9.7, Microsoft SQL Server 2005 & 2008.

The publication entitled RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Guidance Supplement describes the procedures necessary to install and operate RSA Adaptive Authentication in its evaluated configuration.

9 Documentation

The RSA documents provided to the consumer are as follows:

- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Access Management User's Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Authentication Plug-In Developer's Guide;
- Architectural Overview RSA Adaptive Authentication for the Web v6.0.2.1. rev 1.5;
- Best Practices for Challenge Questions;
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Case Management User's Guide;
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Configuration Framework Guide;
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Customer Services Representative;
- (CSR) Administration Guide;
- RSA Diagnostics Manager 3.2 User Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Operations Guide;
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Policy Editor User's Guide;
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Policy Simulator User's Guide;
- Release Notes RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3;
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 Reporting Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Web Services API Reference Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Workflow & Processes Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Integration Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 and RSA FraudAction Bait Credentials;
- Setup and Implementation Guide;

- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP2 Installation Guide;
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Upgrade Guide; and
- RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Guidance Supplement.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of RSA Adaptive Authentication, including the following areas:

Development: The evaluators analyzed RSA Adaptive Authentication 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 RSA Adaptive Authentication security architectural description and determined that the initialization process was secure and 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 were correct.

Guidance Documents: The evaluators examined the RSA Adaptive Authentication preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the RSA Adaptive Authentication configuration management system and associated documentation was performed. The evaluators found that the RSA Adaptive Authentication configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

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

The evaluators reviewed the flaw remediation procedures used by RSA for RSA Adaptive Authentication. 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 RSA Adaptive Authentication. 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 RSA Adaptive Authentication in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 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 found it 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.

The evaluators visited the RSA development site and reviewed their test environment.

11.2 Independent Functional Testing

During this evaluation, the evaluators 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 was the following list of EWA-Canada test goals:

- 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;
- 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;
- Identification and Authentication: The objective of this test goal is to ensure that the TOE identification and authentication requirements operate as specified; and
- User Data protection: The objective of this test goal is to ensure the TOE's data is protected through the Case Risk Engine.

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 Scanning, Direct Attacks, and misuse.

[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.

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

11.4 Conduct of Testing

RSA Adaptive Authentication 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 Procedures and Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that RSA Adaptive Authentication behaves as specified in its ST and functional specification.

12 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.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for RSA Adaptive Authentication includes comprehensive Evaluation, Installation, and Users Guides.

The developer has an extensive and robust test suite capable of insuring a proper working product.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Hash based Message Authentication Code
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories Canada
PRNG	Pseudo Random Number Generator
SHA	Secure Hash Algorithm
SFR	Security Functional Requirement

Acronym/Abbreviation/ Initialization	Description
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Triple Data Encryption Standard
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

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 3.1R3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1R3, July 2009.

d. RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Security Target, 0.5, 31 March 2011.

e. Evaluation Technical Report (ETR) for EAL 2+ Common Criteria Evaluation of RSA Adaptive Authentication System v6.0.2.1 SP3, Document No. 1668-000-D002, Version 1.3, 31 March 2011, Common Criteria Evaluation Number: 383-4-166.